Novell®
Sentinel™

5.1.3

www.novell.com

Volume II – GUIDA DELL'UTENTE DI SENTINEL

7 luglio 2006

Novell®

Note legali

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Documentazione in linea: Per accedere alla documentazione in linea per questo e altri prodotti Novell e per ottenere aggiornamenti, visitare il sito Novell all'indirizzo www.novell.com/documentation.

Marchi di fabbrica Novell

Per i marchi Novell, vedere l'elenco disponibile all'indirizzo (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiali di terze parti

Tutti i marchi di fabbrica di terze parti appartengono ai rispettivi proprietari.

Note legali di terze parti

In Sentinel 5 possono essere incluse le tecnologie di terze parti seguenti:

- Apache Axis e Apache Tomcat, Copyright © 1999-2005, Apache Software Foundation. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.apache.org/licenses/
- ANTLR. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.antlr.org
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.bouncycastle.org.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, pacchetto di utility. Copyright © Doug Lea. Utilizzato senza classi CopyOnWriteArrayList e ConcurrentReaderHashMap.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, con i materiali protetti da copyright seguenti: mars.cpp di Brian Gladman e Sean Woods. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.eskimo.com/~weidai/License.txt.
- Crystal Reports Developer e Crystal Reports Server. Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991-2003.
- edpFTPj, concesso in licenza in base alla GNU Lesser General Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, concesso in licenza in base alla Lesser General Public License disponibile all'indirizzo: http://shark.objectweb.org/license.html.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003-2004.
- ILOG, Inc. Copyright © 1999-2004.
- Installshield Universal. Copyright © 1996-2005, Macrovision Corporation e/o Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt (in lingua inglese).

  Java 2 Platform può inoltre includere i prodotti di terze parti seguenti:

  - CoolServlets © 1999
  - DES and 3xDES © 2000 by Jef Poskanzer
  - Crimson © 1999-2000 The Apache Software Foundation
  - Xalan J2 © 1999-2000 The Apache Software Foundation
  - NSIS 1.0j © 1999-2000 Nullsoft, Inc.

- Tinyxml. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://grinninglizard.com/tinyxmldocs/index.html.
-
- Xalan e Xerces, entrambi concessi in licenza da Apache Software Foundation Copyright © 1999-2004. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo http://xml.apache.org/dist/LICENSE.txt (in lingua inglese).
-

NOTA: Al momento della pubblicazione della presente documentazione i collegamenti indicati sopra risultano attivi. Qualora i collegamenti risultassero non più validi o le relative pagine Web non più attive, contattare Security's Office of the Counsel at 404 Gallows Road, Vienna, VA 500. 703-852-8000.

Prefazione

La documentazione tecnica di Sentinel contiene informazioni generali sull'utilizzo e rappresenta una guida di riferimento. La presente documentazione è rivolta ai professionisti della protezione delle informazioni. Il testo contenuto nella presente documentazione è da considerarsi come documento di riferimento del sistema di gestione della protezione aziendale di Sentinel. Sul portale Web di Novell sono disponibili altri documenti.

La documentazione tecnica di Sentinel è suddivisa in cinque differenti volumi, ovvero:

- Volume I: Guida all'installazione di Sentinel™ 5
- Volume II: Guida dell'utente di Sentinel™ 5
- Volume III: Guida dell'utente di Sentinel™ 5 Wizard
- Volume IV: Guida di riferimento dell'utente di Sentinel™ 5
- Volume V: Guida all'integrazione con soluzioni di terze parti di Sentinel™

Volume I: Guida all'installazione di Sentinel

In questa guida viene descritto come installare i prodotti seguenti:

- Server Sentinel
- Console Sentinel
- Motore di correlazione di Sentinel
- Crystal Reports per Sentinel
- Generatore servizi di raccolta di Wizard
- Gestione servizi di raccolta di Wizard
- Advisor

Volume II: Guida dell'utente di Sentinel

In questa guida vengono descritti gli argomenti seguenti:

- Operazione della console Sentinel
- Funzioni di Sentinel
- Architettura di Sentinel
- Comunicazione di Sentinel
- Arresto/Avvio di Sentinel
- Valutazione delle vulnerabilità
- Monitoraggio degli eventi
- Filtro degli eventi
- Correlazione degli eventi
- Gestione dati Sentinel
- Configurazione eventi per rilevanza aziendale
- Servizio di mappatura
- Rapporti cronologici
- Gestione di host Wizard
- Casi
- Situazioni
- Gestione utenti
- Workflow

Volume III: Guida dell'utente di Wizard

In questa guida vengono descritti gli argomenti seguenti:

- Funzionamento di Generatore servizi di raccolta di Wizard
- Gestione servizi di raccolta di Wizard
- Servizi di raccolta
- Gestione di host Wizard
- Creazione e mantenimento di Servizi di raccolta

Volume IV: Guida di riferimento dell'utente di Sentinel

In questa guida vengono descritti gli argomenti seguenti:

- Linguaggio di script di Wizard
- Comandi di analisi sintattica di Wizard
- Funzioni dell'amministratore di Wizard
- Tag META di Wizard e Sentinel
- Motore di correlazione di Sentinel
- Autorizzazioni utente
- Opzioni della riga di comando di correlazione
- Schema database Sentinel

Volume V: Guida all'integrazione con soluzioni di terze parti di Sentinel

- Remedy
- HP OpenView Operations
- HP Service Desk

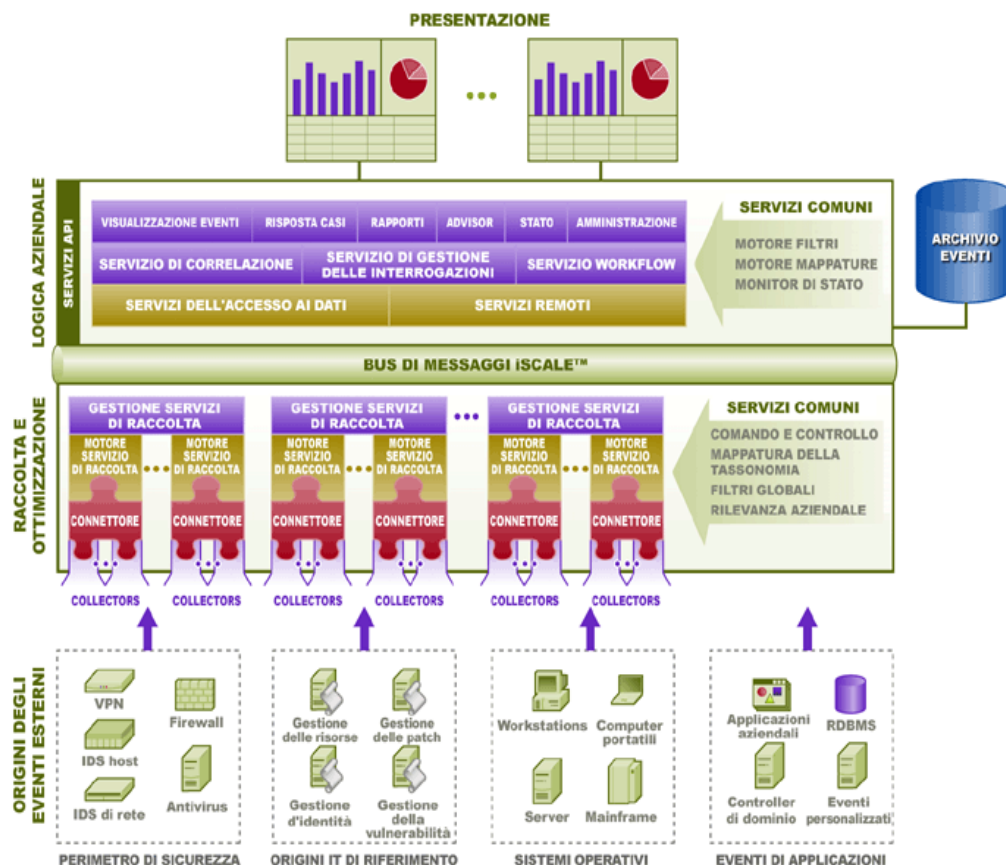
Sommario

1 Introduzione a Sentinel

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Sentinel™ 5 è la soluzione leader per il monitoraggio della conformità e la gestione delle informazioni di sicurezza che riceve informazioni raccolte da molte fonti all'interno di un'azienda, le standardizza, assegna le priorità ed esegue la correlazione in tempo reale. Sentinel raccoglie i dati trasmessi da molti prodotti di sicurezza presenti sul mercato e garantisce la flessibilità necessaria per raccogliere dati da nuove tecnologie e prodotti contestualmente all'evoluzione delle installazioni e alle esigenze dell'azienda.

Molte delle funzionalità offerte da Sentinel 5 sono il risultato di una nuova progettazione a livello di architettura di Sentinel 4.0 e si basano sulle esigenze dei clienti Novell. Poiché si registra un aumento delle minacce alla sicurezza e una maggiore pressione normativa, le aziende sono alla ricerca di una soluzione che consenta loro di:

- Ottenere la visibilità e le conoscenze necessarie per gestire un ambiente di sicurezza in maniera più efficiente in termini di costo.
- Monitorare costantemente la conformità con le politiche interne e le normative legali (ad esempio, Sarbanes-Oxley, HIPAA, GLBA, FISMA, NISPOM, DCID 6/3 e DITSCAP).
- Identificare e risolvere i casi in modo più rapido e più efficiente in termini di costo mediante attività di raccolta e risoluzione automatizzate e centralizzate delle minacce e dei dati sulle norme.
- Fornire sistemi di valutazione operativi ed esecutivi per valutare costantemente lo stato di sicurezza e conformità e raggiungere gli obiettivi strategici e tattici.
- Ridurre i costi operativi associati al monitoraggio della sicurezza e della conformità, all'identificazione dei casi e delle misure di risposta.

Un evento è un'azione oppure occorrenza segnalata a Sentinel. Un evento ricevuto da un dispositivo di sicurezza viene chiamato evento esterno, mentre un evento generato da Sentinel viene chiamato evento interno. Gli eventi possono essere legati alla sicurezza, alle prestazioni o alle informazioni. Un evento esterno, ad esempio, potrebbe essere un attacco rilevato da un sistema di rilevamento delle intrusioni (IDS), un login avvenuto correttamente segnalato da un sistema operativo o da una situazione definita da un cliente, ad esempio l'apertura di un file da parte di un utente. Gli eventi interni sono generati da Sentinel per segnalare un cambiamento significativo allo stato del sistema, ad esempio l'arresto di un servizio di raccolta o la disattivazione di una regola di correlazione.

La correlazione è il processo di analisi degli eventi di sicurezza per identificare gli schemi all'interno di un evento o di un flusso di eventi. Ad esempio, è possibile creare una regola di correlazione per rilevare quando si verificano trenta o più eventi ICMP in un intervallo di tempo di un minuto. Il traffico ad alto volume (inondazione) di ICMP potrebbe indurre un attacco Denial of Service. La correlazione può rilevare gli schemi in un flusso di eventi da un singolo dispositivo, una serie di dispositivi analoghi o una raccolta arbitraria di dispositivi. Ciò consente all'utente di determinare in modo più preciso il livello di rischio e la gravità del caso.

In Sentinel sono inoltre integrate altre informazioni, ad esempio informazioni sui computer della rete e i relativi servizi noti e le vulnerabilità. Queste informazioni sono messe a disposizione in tempo reale rifinendo la rilevanza degli eventi sottoposti al monitoraggio.

Sentinel Control Center utilizza processi in background per visualizzare eventi in tempo reale e riepiloghi di eventi (Active Views™), Casi, rapporti cronologici (Analisi) e rapporti Advisor.

Gli eventi considerati di importanza significativa possono essere raggruppati insieme in un oggetto chiamato *Caso*. I casi possono essere creati manualmente dall'utente oppure automaticamente dal motore di correlazione. Nel caso possono essere contenute informazioni aggiuntive, ad esempio informazioni sulle risorse interessate, sulle vulnerabilità di tali risorse e informazioni sull'attacco recuperate dal componente Sentinel Advisor. È inoltre possibile includere altre informazioni sotto forma di allegati.

In questa guida si presume che l'utente abbia familiarità con le nozioni di base di sicurezza di rete, l'amministrazione dei database e i sistemi operativi Windows e UNIX.

In questo capitolo viene descritta l'architettura funzionale e logica di Sentinel 5, seguita dai moduli chiave del prodotto.

Architettura funzionale

Sentinel 5 si compone di tre sottosistemi componente, che costituiscono il fulcro dell'architettura funzionale:

- Piattaforma iSCALE: un framework scalabile basato su eventi
- Integrazione dell'origine dati: un framework di servizi di raccolta estendibile
- Integrazione dell'applicazione: un framework di applicazione estendibile

Sentinel tratta sia i “servizi” che le “applicazioni” come endpoint di servizi astratti che riescono a rispondere tempestivamente ad eventi asincroni. I servizi sono “oggetti” che non devono capire i protocolli o le modalità di instradamento dei messaggi ai servizi peer.

Funzioni di Sentinel

Sentinel è un'applicazione per l'utente finale ricca di funzionalità che consente di monitorare e gestire una serie di funzioni. Alcune delle funzioni principali:

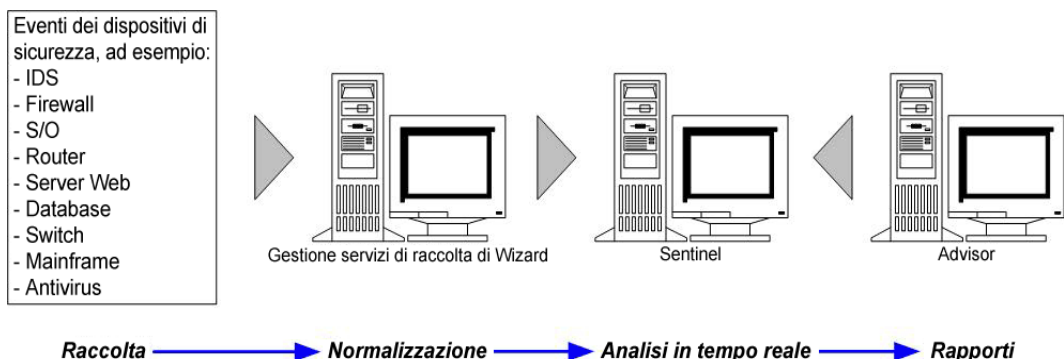
- Fornisce visualizzazioni in tempo reale di ampi flussi di eventi
- Offre capacità di esecuzione di rapporti sulla base di eventi cronologici non in tempo reale
- Regola gli utenti e ciò che sono in grado di visualizzare e fare mediante l'assegnazione delle autorizzazioni
- Consente di limitare l'accesso agli eventi da parte degli utenti
- Consente di organizzare gli eventi in casi per garantire una gestione efficace della risposta e il controllo
- Consente di rilevare gli schemi negli eventi e i flussi di eventi

Panoramica dell'architettura

Il sistema Sentinel è responsabile della ricezione degli eventi da Gestione servizi di raccolta di Wizard. Gli eventi sono successivamente visualizzati in tempo reale e connessi a un database per l’analisi cronologica.

A livello elevato, il sistema Sentinel utilizza un database relazionale e si compone di processi Sentinel e di un motore di esecuzione dei rapporti. Il sistema accetta gli eventi da Gestione servizi di raccolta come input, che interfaccia con prodotti di terze parti e normalizza i dati

inviati da questi prodotti. I dati normalizzati sono quindi inviati ai processi Sentinel e al database.

L'analisi cronologica e dei rapporti può essere eseguita mediante il motore di esecuzione dei rapporti integrato di Sentinel. Il motore di esecuzione dei rapporti estrae i dati dal database e integra le visualizzazioni dei rapporti in Sentinel Control Center utilizzando i documenti HTML mediante una connessione HTTP.

Le funzioni di Sentinel sono le seguenti:

- Elaborazione in tempo reale degli eventi ricevuti da Gestione servizi di raccolta di Wizard
- Un linguaggio per la correlazione intuitivo e flessibile basato sulle regole
- Regole compilate per prestazioni elevate
- Architettura scalabile, multi-threaded, distribuibile ed estendibile

I processi Sentinel comunicano tra di loro mediante un middleware di messaggistica (MOM).

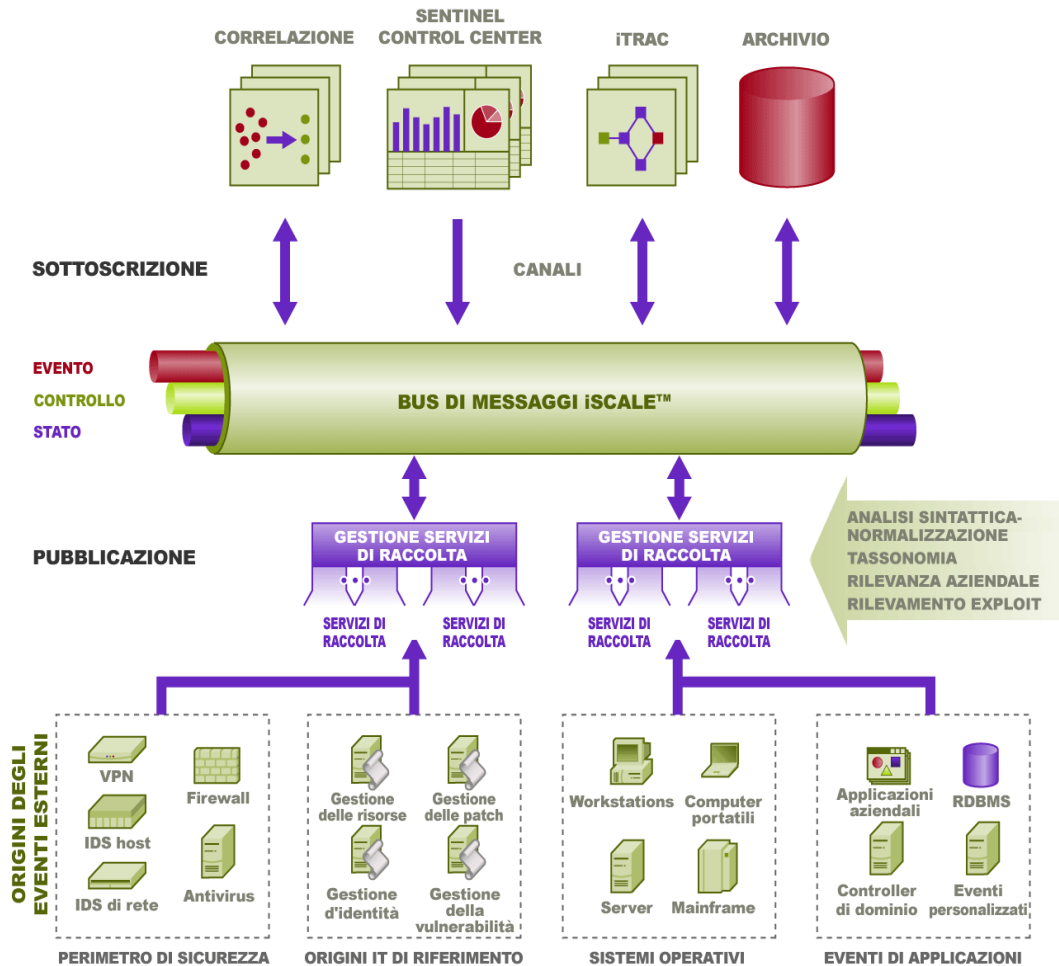
Piattaforma iSCALE

L'architettura iSCALE™ di Sentinel è creata sulla base di un'architettura basata su standard e orientata ai servizi (SOA) che associa i vantaggi dell'elaborazione in memoria all'elaborazione distribuita. Il fulcro di iSCALE è rappresentato da un bus di messaggi specializzato in grado di gestire elevati volumi di dati. Realizzato dal nulla utilizzando l'approccio migliore basato sugli standard, iSCALE è in grado di scalare in modo efficace in termini di costo.

Bus messaggi

Il bus messaggi iSCALE consente di scalare in modo indipendente i singoli componenti e allo stesso tempo di eseguire un'integrazione basata sugli standard con le applicazioni esterne. La chiave della scalabilità risiede nel fatto che, diversamente da altro software distribuito, due componenti peer non comunicano mai tra di loro in modo diretto. Tutti i componenti comunicano mediante il bus messaggi, il quale è in grado di spostare migliaia di pacchetti di messaggi al secondo.

Sfruttando le incredibili capacità del bus messaggi, il canale di comunicazione a elevata capacità di trasmissione riesce a ridurre al minimo e a sostenere una elevata frequenza di trasmissione dei dati lungo i componenti indipendenti del sistema. Gli eventi sono compressi e cifrati via cavo per garantire una consegna sicura ed efficiente dal bordo della rete o dai punti di raccolta all'hub del sistema, dove vengono eseguite analisi in tempo reale.

Il bus messaggi iSCALE utilizza una serie di servizi per inviare i messaggi in coda che migliorano l'affidabilità delle comunicazioni al di la degli aspetti di sicurezza e delle prestazioni della piattaforma. Mediante una serie di code transitorie e durature, il sistema garantisce un'affidabilità e una tolleranza agli errori senza paragoni. Ad esempio, i messaggi importanti in transito sono salvati (inserendoli in coda) in caso di errore nel percorso di comunicazione. Il messaggio in coda viene inviato a destinazione solo dopo aver risolto l'errore di sistema.

Canali

La piattaforma iSCALE utilizza un modello basato sui dati o sugli eventi che consente di scalare in modo indipendente i componenti dell'intero sistema in base al carico di lavoro. Ciò garantisce un modello di distribuzione flessibile poiché l'ambiente di ogni cliente varia: un sito potrebbe avere un numero molto ampio di dispositivi con volumi di eventi bassi, mentre un altro sito potrebbe avere un numero minore di dispositivi con volumi maggiori di eventi. In questi casi, le densità dell'evento (ovvero l'aggregazione dell'evento e lo schema multiplexing dell'evento via cavo dai punti di raccolta) sono differenti e il bus messaggi consente di scalare in modo coerente i diversi carichi di lavoro.

iSCALE sfrutta un ambiente indipendente con canali multipli che elimina qualsiasi contenzioso e incoraggia l'elaborazione parallela degli eventi. Questi canali e sottocanali non

lavorano solo per il trasporto dei dati relativi agli eventi ma offrono inoltre un controllo accurato dei processi per scalare e bilanciare il carico del sistema in varie condizioni di carico. L'utilizzo di canali di servizio indipendenti, ad esempio canali di controllo e di stato, in aggiunta al principale canale degli eventi, consente di scalare in modo sofisticato ed efficace in termini di costo l'architettura basata sugli eventi.

Evento Sentinel

Sentinel riceve informazioni dai dispositivi, le normalizza in una struttura chiamata *Evento Sentinel* o semplicemente *Evento* e inviano l'evento ai fini dell'elaborazione. Gli eventi sono elaborati dalla visualizzazione in tempo reale, dal motore di correlazione e dal server backend.

Un evento comprende oltre 200 tag. I tag sono di diverso tipo e hanno scopi differenti. Esistono alcuni tag predefiniti, ad esempio la gravità, la criticità, l'indirizzo IP di destinazione e la porta di destinazione. Esistono due tipi di tag configurabili: Tag riservati per uso interno Novell per consentire la futura espansione e i tag utente per le estensioni degli utenti.

Lo scopo dei tag può essere modificato mediante il processo di ridenominazione. L'origine di un tag può essere *esterna*, ovvero impostata in modo esplicito dal dispositivo o dal servizio di raccolta corrispondente, oppure *referenziale.* Il valore di un tag referenziale viene elaborato come una funzione di uno o più tag differenti che utilizzano il servizio di mappatura. Ad esempio, è possibile definire un tag come il codice di creazione per la creazione contenente la risorsa indicata come IP di destinazione di un evento. Ad esempio, un tag può essere elaborato dal servizio di mappatura utilizzando una mappa definita dal cliente utilizzando l'IP di destinazione inviato dall'evento.

Servizio di mappatura

Il Servizio di mappatura consente a un meccanismo sofisticato di diffondere i dati di rilevanza aziendale in tutto il sistema. Questa struttura facilita la scalabilità e offre vantaggi notevoli abilitando il trasferimento di dati intelligenti tra nodi differenti del sistema distribuito.

Il Servizio di mappatura è una struttura di propagazione dei dati che offre la possibilità di effettuare riferimenti incrociati tra i dati relativi alla scansione delle vulnerabilità e le firme dei sistemi di rilevamento delle intrusioni (ad esempio, dati sulle risorse, dati relativi all'azienda e così via). Ciò consente di ricevere una notifica immediata quando un attacco cerca di penetrare in un sistema vulnerabile. Questa funzionalità è garantita da tre componenti distinti:

- Raccolta di eventi in tempo reale da un'origine di rilevamento delle intrusioni;
- Confronto tra le suddette firme e le scansioni delle vulnerabilità più recenti; e
- riferimento incrociato di un feed relativo agli attacchi mediante Sentinel Advisor (modulo del prodotto opzionale, che esegue riferimenti incrociati tra firme sull'attacco IDS in tempo reale e i dati relativi alla scansione delle vulnerabilità dell'utente).

Il Servizio di mappatura propaga in modo dinamico le informazioni in tutto il sistema senza ripercuotersi sul carico del sistema. Quando nel sistema vengono aggiornate importanti serie di dati (ad esempio, "mappe" relative a informazioni sulle risorse o informazioni di aggiornamento della patch), il Servizio di mappatura distribuisce l'aggiornamento nel sistema, con dimensioni, a volte, superiori a centinaia di megabyte.

Gli algoritmi del Servizio di mappatura di iSCALE gestiscono ampie serie di dati referenziali all'interno di un sistema di produzione che elabora grandi volumi di dati in tempo reale. Questi algoritmi sono in grado di riconoscere gli aggiornamenti e spingono in modo selettivo solo le modifiche o le "serie di dati delta" dall'archivio al bordo o al perimetro del sistema.

Streaming delle mappe

Il Servizio di mappatura utilizza un modello di aggiornamento dinamico ed esegue lo streaming delle mappe da un punto all'altro, evitando la creazione di mappe dinamiche di grandi dimensioni nella memoria dinamica. L'importanza della capacità di streaming è particolarmente rilevante in un sistema in tempo reale mission-critical, ad esempio quello di Sentinel dove è necessario un movimento costante, prevedibile e veloce dell'indipendenza dei dati di qualsiasi carico transitorio sul sistema.

Rilevamento degli exploit (Servizio di mappatura)

Sentinel consente di eseguire riferimenti incrociati tra le firme dei dati relativi agli eventi e i dati della scansione delle vulnerabilità. Ciò consente di inviare una notifica immediata e automatica agli utenti quando un attacco cerca di penetrare in un sistema vulnerabile. Tale funzionalità è garantita da:

- feed di dati di Advisor
- rilevamento delle intrusioni
- scansione delle vulnerabilità
- Firewall

In Advisor è incluso un riferimento incrociato tra le firme dei dati relativi agli eventi e i dati relativi alla scansione delle vulnerabilità. In Advisor sono disponibili feed di dati per avvisi e attacchi. Nel feed relativo agli attacchi sono contenute informazioni sulle vulnerabilità e le minacce. Il feed relativo agli attacchi è una normalizzazione delle firme relative agli eventi e dei plug-in delle vulnerabilità. Per informazioni sull'installazione di Advisor, vedere la Guida all'installazione di Sentinel.

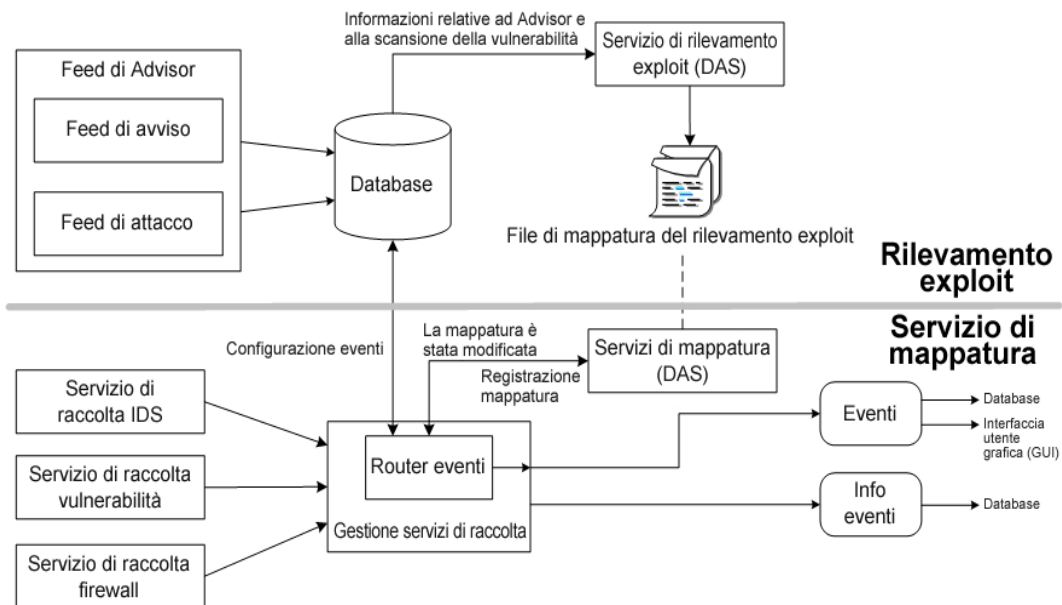
I sistemi supportati sono i seguenti:

Sistemi di rilevamento delle intrusioni
- Cisco Secure IDS
- Enterasys Dragon Host Sensor
- Enterasys Dragon Network Sensor
- Intrusion.com (SecureNet_Provider)
- ISS BlackICE
- ISS RealSecure Desktop
- ISS RealSecure Network
- ISS RealSecure Server
- ISS RealSecure Guard
- Snort
- Symantec Network Security 4.0 (ManHunt)
- Symantec Intruder Alert
- McAfee IntruShield

Scansioni delle vulnerabilità
- eEYE Retina
- Foundstone Foundscan
- ISS Database Scanner
- ISS Internet Scanner
- ISS System Scanner
- ISS Wireless Scanner
- Nessus
- nCircle IP360
- Qualys QualysGuard

Firewall
- Cisco IOS Firewall

Sarà necessario almeno una scansione delle vulnerabilità e un IDS o un firewall delle categorie illustrate sopra. L'IDS o DeviceName (rv31) Firewall deve essere visualizzato nell'evento come evidenziato in grigio sopra. L'IDS e il Firewall devono inoltre inserire i dati in modo corretto nel campo DeviceAttackName (rt1) (ad esempio, l'accesso WEB-PHP Mambo uploadimage.php).

Il feed di dati di Advisor viene inviato al database e successivamente al servizio di rilevamento degli exploit. Il servizio di rilevamento degli exploit genererà uno o due file, in base al tipo di dati aggiornati.

Il Servizio di mappatura utilizza i file delle mappe prodotti dal rilevamento degli exploit per mappare gli attacchi agli exploit delle vulnerabilità.

Le scansioni delle vulnerabilità eseguono la ricerca delle aree vulnerabili (risorsa) del sistema. IDS rileva gli (eventuali) attacchi contro tali aree vulnerabili. I Firewall rilevano eventuale traffico contro tali aree vulnerabili. Se un attacco è associato a una vulnerabilità, la risorsa è stata sfruttata.

Il servizio di rilevamento degli exploit genera due file nel percorso seguente:

```
$ESEC_HOME/sentinel/bin/map_data
```

I due file sono attackNormalization.csv ed exploitDetection.csv.

Il file attackNormalization.csv è generato dopo

- Feed di dati di Advisor
- Avvio di DAS (se attivato in das_query.xml, disattivato per default)

Il file exploitDetection.csv viene generato dopo uno dei seguenti:

- Feed di dati di Advisor
- Scansione delle vulnerabilità
- Avvio del server Sentinel (se attivato in das_query.xml, disattivato per default)

Per default, sono disponibili due colonne eventi già configurate utilizzate per il rilevamento degli exploit e che fanno riferimento a una mappa (a tutti i tag mappati sarà associata un'icona di scorrimento).

- Vulnerability (vulnerabilità)
- AttackId

Severity	Vulnerability	AttackId
2	0	
3	0	

Se il valore nel campo della vulnerabilità *(vul)* è pari a 1, la risorsa o il dispositivo di destinazione viene utilizzato. Se invece il valore nel campo Vulnerabilità è pari a 0, significa che la risorsa o il dispositivo di destinazione non è sfruttato.

Sentinel è pre-configurato con i nomi delle mappe seguenti associati ai file attackNormalization.csv ed exploitDetection.csv.

Nome mappa	Nome file csv
▪ AttackSignatureNormalization	▪ attackNormalization.csv
▪ IsExploitWatchlist	▪ exploitDetection.csv

Esistono due tipi di origini dati:

- Esterno: recupera le informazioni dal servizio di raccolta
- Riferimento da mappatura: le informazioni vengono recuperate da un file di mappatura al fine di inserire i dati nel tag.

Il tag AttackId ha le colonne Device (tipo del dispositivo di sicurezza, ad esempio Snort) e AttackSignature impostate come chiavi e utilizza la colonna NormalizedAttackID nel file attackNormalization.csv. In una riga dove il tag evento DeviceName (un dispositivo IDS, ad esempio, Snort, informazioni inserite da Advisor e informazioni sulle vulnerabilità inviate dal database di Sentinel) è uguale a Device e il tag evento DeviceAttackName (informazioni sull'attacco inserite dalle informazioni di Advisor nel database di Sentinel mediante il servizio di rilevamento degli exploit) è uguale ad AttackSignature, il valore di AttackId è fornito dall'intersezione della riga con la colonna NormalizedAttackID.

Nel tag Vulnerability (vulnerabilità) è presente la voce di colonna "_EXIST_", che indica che il valore del risultato della mappatura sarà 1 se la chiave si trova in IsExploitWatchlist (file exploitDetection.csv) oppure 0 in caso contrario. Le colonne chiave per il tag delle vulnerabilità sono IP e NormalizedAttackId. Quando un evento in ingresso con un tag evento

DestinationIP corrisponde alla voce della colonna IP e un tag evento AttackId corrisponde alla voce della colonna NormalizedAttackId nella stessa riga, il risultato è uno (1). Se in una riga comune non viene rilevata alcuna corrispondenza, il risultato è zero (0).

Integrazione dell'origine dei dati

L'utilizzo di una tecnologia adattabile e flessibile è fondamentale per la strategia di integrazione dell'origine dei dati di Sentinel, ottenuta mediante servizi di raccolta interpretativi (chiamati anche servizi di raccolta) che analizzano e normalizzano gli eventi nel flusso di dati.

Questi servizi di raccolta possono essere modificati in base alle esigenze e non sono legati a un ambiente specifico. Le attività di creazione, modifica, distribuzione e manutenzione dei servizi di raccolta sono molto semplici e possono essere eseguite direttamente dagli utenti. Un ambiente di sviluppo integrato consente la creazione di servizi di raccolta mediante l'utilizzo di un'opzione “trascina e rilascia selezione” di un'interfaccia utente grafica. Gli utenti non programmatori possono creare servizi di raccolta, in modo da garantire che le richieste attuali e future in un ambiente IT in continua evoluzione siano sempre soddisfatte. I comandi e le operazioni di controllo dei servizi di raccolta (ad esempio, avvio o arresto) sono eseguiti a livello centrale da Sentinel Control Center.

Integrazione dell'applicazione

L'integrazione delle applicazioni esterne mediante API standard è fondamentale per Sentinel. Ad esempio, un API bidirezionale per i sistemi di ticketing dei problemi tra cui Remedy® e HP OpenView’s ServiceDesk® consente di eseguire un'integrazione immediata con i sistemi esterni.

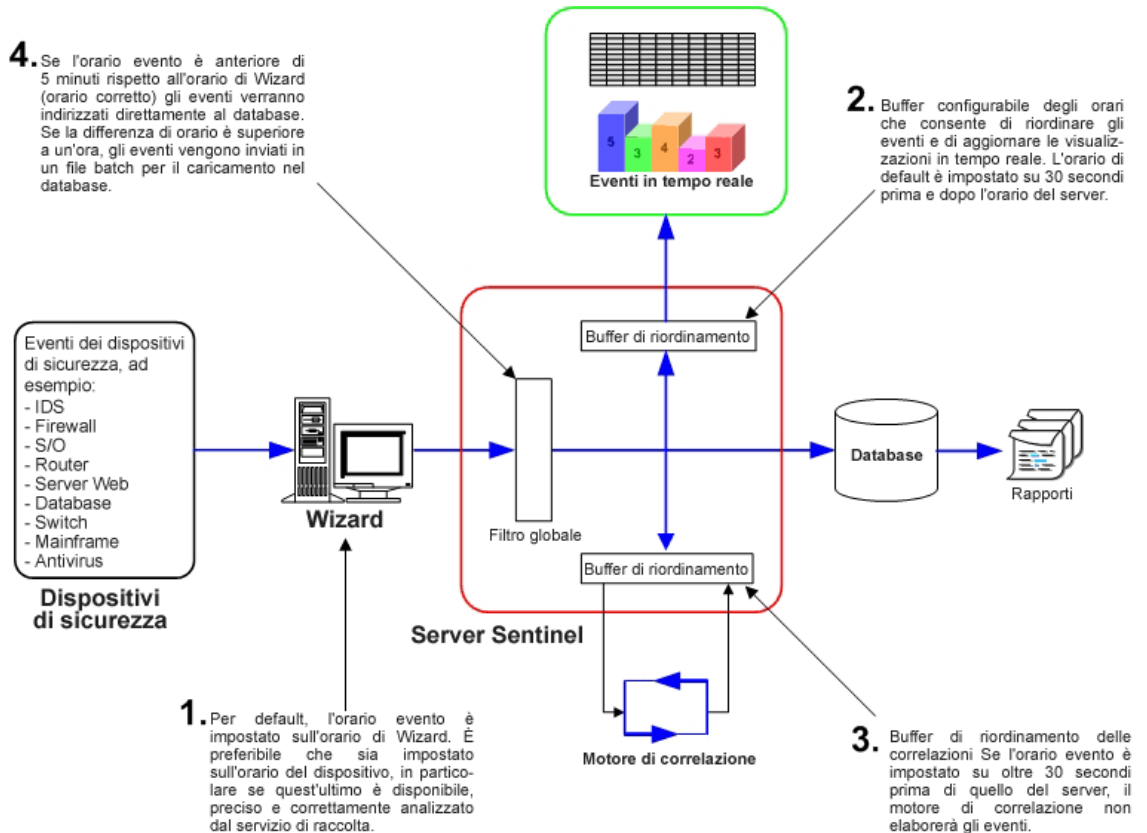
L'API si basa sui Servizi Web e, pertanto, consente a qualsiasi sistema esterno sensibile a SOAP di sfruttare l'integrazione diffusa con il sistema Sentinel.

Ora

L'ora di un evento è un elemento critico per la relativa elaborazione. È importante inoltre ai fini della generazione dei rapporti e delle verifiche, nonché dell'elaborazione in tempo reale. Il motore di correlazione elabora i flussi di eventi ordinati per ora e rileva gli schemi

all'interno degli eventi e gli schemi temporali nel flusso. Tuttavia, il dispositivo che genera l'evento potrebbe non essere a conoscenza dell'ora effettiva in cui l'evento è stato generato. Per poter risolvere questo problema, in Sentinel sono disponibili due opzioni per l'elaborazione degli avvisi inviati dai dispositivi di sicurezza: considerare come valida l'ora indicata dal dispositivo e utilizzarla come l'ora dell'evento, oppure non considerare valida l'ora del dispositivo e archiviare l'evento all'ora in cui è stato elaborato per la prima volta da Sentinel (dal servizio di raccolta).

Sentinel è un sistema distribuito e comprende diversi processi che possono trovarsi in differenti parti della rete. Il dispositivo potrebbe inoltre indurre alcuni ritardi. Per risolvere questo problema, i processi Sentinel riorganizzano gli eventi in un flusso ordinato in base all'ora prima di elaborarli.

Nell'illustrazione seguente è descritto il concetto dell'Ora di Sentinel.

1. Per default, l'Orario evento è impostato sull'ora di Wizard. L'orario ideale sarebbe quello del dispositivo. Pertanto, sarebbe opportuno impostare l'orario evento sull'orario dispositivo, se questo è disponibile, preciso e sottoposto a corretta analisi dal servizio di raccolta.
2. Un buffer orario configurabile che riordina gli eventi e aggiorna le visualizzazioni in tempo reale. L'orario di default è 30 secondi in anticipo e in ritardo rispetto all'orario del server.
3. Buffer di riordinamento della correlazione, se l'orario dell'evento è superiore a 30 secondi rispetto all'orario del server. Il motore di correlazione non elaborerà gli eventi.

4. Se l'orario dell'evento è superiore a 5 minuti rispetto all'orario di Wizard (orario corretto), gli eventi saranno instradati direttamente al database.

Eventi interni o di sistema

Gli eventi interni o di sistema consentono di fornire rapporti sullo stato del sistema e sulle modifiche a esso apportate. Il sistema interno può generare due tipi di eventi, ovvero:

- Eventi interni
- Eventi di prestazioni

Gli eventi interni sono informativi e descrivono un singolo stato o una modifica allo stato del sistema. Segnalano inoltre quando un utente effettua il login o non riesce a completare l'autenticazione e indicano l'avvio di un processo o l'attivazione di una regola di correlazione. Gli eventi di prestazioni sono generati periodicamente e descrivono le risorse mediamente utilizzate dai diversi componenti del sistema.

Tutti gli eventi di sistema inseriscono dati negli attributi seguenti:

- Campo ST (tipo sensore): per gli eventi interni è impostato su "I", mentre per gli eventi di prestazioni è impostato su "P"
- ID evento: UUID univoco dell'evento
- Orario evento: orario in cui è stato generato l'evento
- Origine: UUID del processo che ha generato l'evento
- Nome del sensore: nome del processo che ha generato l'evento (ad esempio, DAS_Binary)
- RV32 (categoria dispositivo): impostato su "ESEC"
- Servizio di raccolta: "Prestazioni" per gli eventi di prestazioni e "Interno" per gli eventi interni.

In aggiunta agli attributi comuni, in ogni evento di sistema sono inoltre impostate le risorse, le sotto risorse, la gravità, il nome dell'evento e i tag del messaggio. Per gli eventi interni, il nome dell'evento è sufficientemente specifico da identificare il significato esatto dell'evento (ad esempio, UserAuthenticationFailed). I tag del messaggio aggiungono alcuni dettagli specifici. Nel precedente esempio il tag del messaggio contiene il nome dell'utente, il nome del sistema operativo, se disponibile, e il nome del computer. Per gli eventi di prestazioni, il nome dell'evento è generico e descrive il tipo di dati statistici e i dati stessi si trovano nel tag del messaggio.

Gli eventi di prestazioni sono inviati direttamente al database. Per visualizzarli, eseguire un'interrogazione rapida.

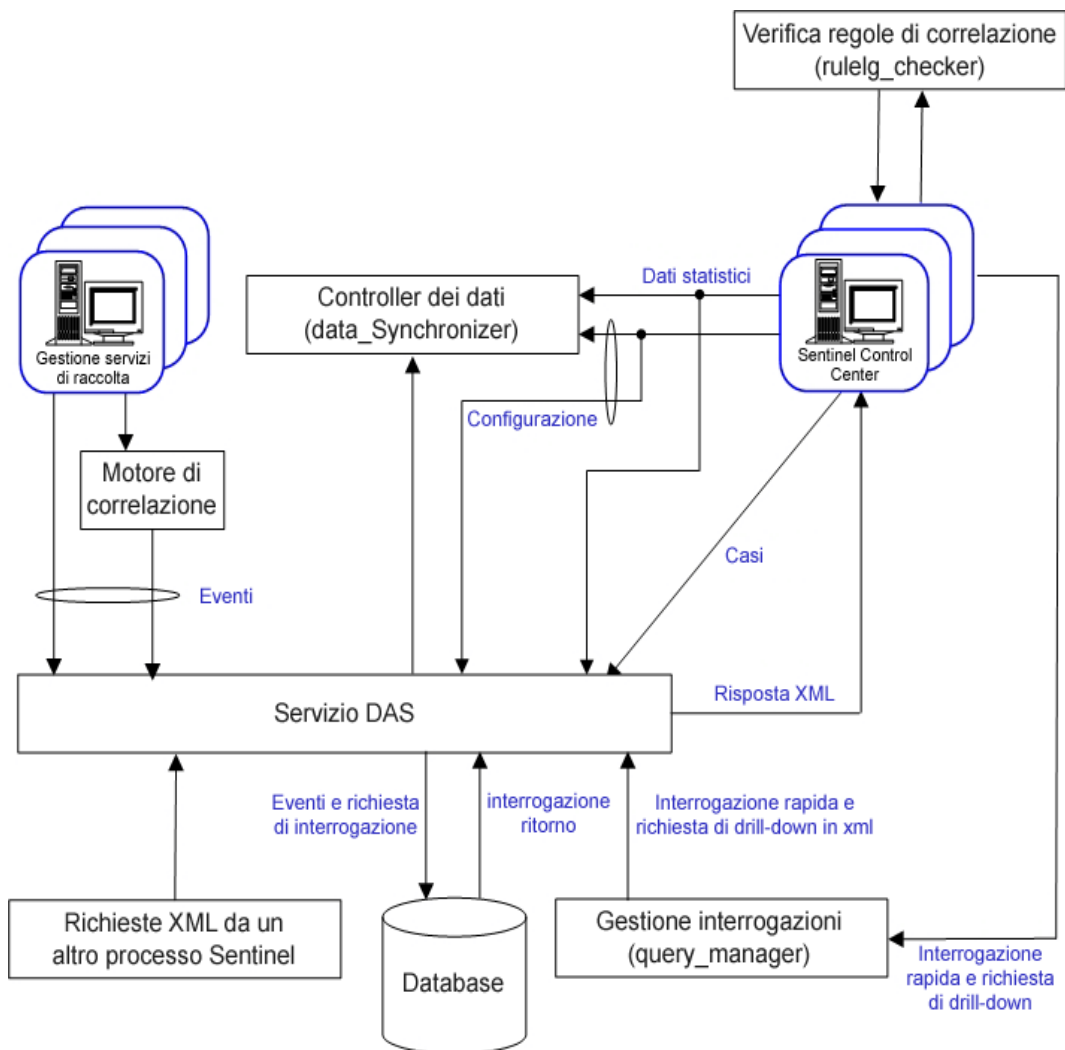
Vedere l'appendice A: Eventi di sistema.

Processi

I processi Sentinel e il servizio di Windows riportati di seguito comunicano tra di loro mediante iSCALE, il middleware di messaggistica (MOM).

- Sorveglianza
- Statistiche evento
- Sincronizzazione dei dati (Controller dei dati)
- Motore di correlazione
- Processo di verifica RuleLg (processo di verifica delle regole di correlazione)
- DAS (Data Access Service) – binario, interrogazione e Active Views™

- Gestione interrogazioni
- Servizio eSecurity (solo MSSQL) – vedere Sorveglianza

La seguente è l'architettura per il server Sentinel.

Processo di sorveglianza

Il processo di sorveglianza di Sentinel consente la gestione di altri processi del server. Se si interrompe un altro processo, il servizio di sorveglianza segnala l'attività e lo riavvia.

Per Windows, la sorveglianza è un servizio chiamato Sentinel. Se questo servizio viene arrestato, interromperà tutti i processi Sentinel in esecuzione sul computer.

Statistiche evento

Il motore delle statistiche sull'evento è un componente del processo das_binary. Gestisce i dati utilizzati dai grafici Active Views e dalle tabelle eventi in Sentinel Control Center.

Il motore conserva una serie di eventi e dati statistici per ciascun filtro e combinazione di attributi degli eventi specificati nel Wizard di Active Views. La prima volta che un utente crea una visualizzazione Active Views con un determinato filtro e attributo evento, viene

creata una nuova serie di dati. Nella serie di dati sono riportati i conteggi dell'attributo a intervalli fissi, oltre agli eventi più recenti per ogni intervallo. Ogni serie di dati è configurata in modo da memorizzare le 24 ore di dati più recenti.

Gli intervalli sono inviati a Sentinel Control Center dopo un breve ritardo, per stabilizzare i dati che potrebbero arrivare in ritardo a causa di ritardi di rete e di orario.

Le visualizzazioni Active Views sono condivise in modo automatico da più utenti se l'attributo evento desiderato e il filtro sono uguali. Quando una visualizzazione Active Views non è più utilizzata da alcun utente, verrà eliminata dopo un'ora. Tuttavia, se viene salvata nelle preferenze dell'utente, la visualizzazione Active Views continuerà a raccogliere dati per 100 ore.

Processo di sincronizzazione dei dati (controller di dati)

Il processo di sincronizzazione dei dati (data_synchronizer) gestisce la modifica dei dati di configurazione da parte di più utenti. Quando un utente richiede di modificare i dati tramite Sentinel Control Center, il record dei dati viene bloccato da data_synchronizer. I dettagli di chi ha bloccato i dati sono pubblicati su altri Sentinel Control Center attivi e nessun altro utente può modificare quei dati. Se un Sentinel Control Center viene chiuso prima che i dati in esso contenuti vengano sbloccati, i dispositivi di bloccaggio non saranno più validi.

Processo del motore di correlazione (correlation_engine)

Il processo del motore di correlazione (correlation_engine) riceve eventi da Gestione servizi di raccolta di Wizard e pubblica eventi correlati in base a regole di correlazione definite dall'utente.

Processo di verifica RuleLg (rulelg_checker)

Il processo di verifica RuleLg (rulelg_checker) consente di convalidare la sintassi dei filtri e le espressioni delle regole di correlazione. Sentinel Control Center utilizza questi risultati per stabilire se sia possibile salvare un filtro o una regola di correlazione.

Processo DAS (Data Access Service)

Il processo DAS (Data Access Service) è il servizio di persistenza del server Sentinel che fornisce un'interfaccia al database. Garantisce l'accesso basato su dati al database backend.

DAS è un container, composto da cinque processi differenti. Ogni processo è responsabile di differenti tipi di operazioni del database. Questi processi sono controllati dai file di configurazione seguenti:

- das_binary.xml: utilizzato per gli eventi e le operazioni di inserimento di eventi correlati
- das_query.xml: tutte le altre operazioni di database
- activity_container.xml: utilizzato per l'esecuzione e la configurazione del servizio di attività
- workflow_container.xml: utilizzato per configurare il servizio del workflow (iTRAC).
- das_rt.xml: utilizzato per la configurazione della funzione Active Views all’interno della console di controllo di Sentinel

Il processo DAS riceve le richieste dai diversi processi Sentinel, le converte in un'interrogazione sul database, elabora il risultato prodotto dal database e lo converte in una risposta. Supporta richieste di recupero di eventi per l'interrogazione rapida e il drill-down, di recupero di informazioni sulle vulnerabilità e su Advisor e di manipolazione delle informazioni di configurazione. Il servizio DAS gestisce inoltre la registrazione di tutti gli

eventi ricevuti da Gestione servizi di raccolta di Wizard e le richieste di recupero e memorizzazione delle informazioni di configurazione.

Gestione delle interrogazioni (query_manager)

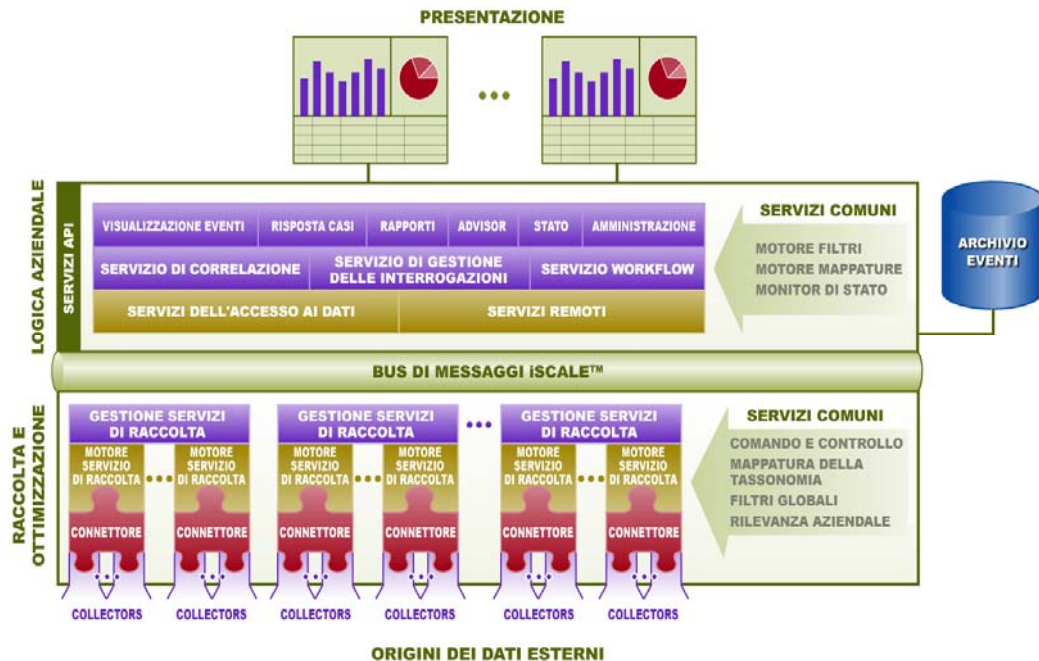
Il servizio di gestione delle interrogazioni (query_manager) riceve richieste di interrogazioni rapide e di drill-down da Sentinel Control Center e le invia al database tramite DAS. Le richieste ricevute da Sentinel Control Center definiscono gli eventi necessari per mezzo di filtri. Se si utilizza un filtro, il servizio di gestione delle interrogazioni ne recupera la definizione e lo converte in un criterio xml. Il servizio di gestione delle interrogazioni invia quindi la richiesta al processo DAS. Non è possibile convertire completamente tutti i filtri in interrogazioni che possono essere elaborate dal database. Se un filtro viene convertito interamente, il servizio di gestione delle interrogazioni indica a DAS di inviare la risposta direttamente a Sentinel Control Center. Se il filtro contiene espressioni regolari che non possono essere convertite in SQL, il servizio di gestione delle interrogazioni effettua le conversioni possibili e genera un criterio conservativo che restituisce un superset degli eventi richiesti. In tal caso, DAS viene istruito a restituire il risultato al servizio di gestione delle interrogazioni. Una volta ricevuta la risposta, il servizio di gestione delle interrogazioni la filtra nella memoria e invia gli eventi che soddisfano le condizioni di filtro a Sentinel Control Center.

Architettura logica

Sentinel 5 si compone di tre strati logici:

- strato di raccolta e di arricchimento
- strato logico aziendale
- strato di presentazione.

Lo strato di raccolta/arricchimento aggrega gli eventi prodotti da origini di dati esterni, trasforma i formati specifici dei dispositivi in formato Sentinel, arricchisce le origini degli eventi nativi con dati di importanza aziendale e distribuisce i pacchetti degli eventi al bus messaggi. Il componente chiave alla base di questa funzione è il servizio di raccolta, coadiuvato da un servizio di mappatura tassonomica e di filtro globale.

Lo strato logico aziendale contiene una serie di componenti distribuibili. Il componente di base è un Servizio remoto che aggiunge capacità di messaggistica agli oggetti di dati e ai servizi per consentire l'accesso trasparente ai dati in tutta la rete e un servizio DAS che è un servizio di gestione degli oggetti che consente agli utenti di definire gli oggetti mediante metadati. Ulteriori servizi comprendono quelli di correlazione, gestione interrogazioni, workflow, visualizzazione eventi, risposta ai casi, stato, Advisor, rapporti e amministrazione.

Al livello di presentazione viene eseguito il rendering dell'interfaccia dell'applicazione per l'utente finale. Un dashboard esaustivo chiamato Sentinel Control Center offre un workbench utente integrato costituito da una serie di sette applicazioni differenti accessibili da un unico framework comune. Questo framework a piattaforma incrociata è creato sulla base degli standard Java™ 1.4 e offre una visione unificata dei componenti logici aziendali indipendenti: grafici interattivi in tempo reale, risposta ai casi eseguibile, workflow dei casi automatizzato e applicabile, generazione di rapporti, misure di risposta contro exploit noti e molto altro ancora.

Ogni strato è illustrato nella figura precedente e illustrato in dettaglio nelle sezioni seguenti.

Strato di raccolta e di arricchimento

Gli eventi sono aggregati mediante una serie di servizi di raccolta flessibili e configurabili che raccolgono dati da una incredibile quantità di sensori e altri dispositivi e fonti. Gli utenti possono utilizzare servizi di raccolta preesistenti, modificare i servizi di raccolta o creare servizi di raccolta personalizzati allo scopo di garantire che il sistema soddisfi tutti i requisiti.

I dati aggregati dai servizi di raccolta sotto forma di eventi sono successivamente normalizzati e trasformati in formato XML, arricchiti con una serie di metadati (ad esempio, dati sui dati) mediante una serie di servizi di rilevanza aziendale e propagati al lato server per un'ulteriore analisi di elaborazione mediante una piattaforma del bus messaggi. Lo strato di raccolta e arricchimento è costituito dai componenti seguenti:

- Connettori e servizio di raccolta
- Motore e Gestione servizi di raccolta
- Generatore servizi di raccolta

Connettori e servizi di raccolta

Un Connettore è un concentratore o una scheda multiplexed che collega il motore dei servizi di raccolta ai dispositivi effettivamente monitorati.

I servizi di raccolta sono l'elemento di aggregazione a livello di componente dei dati dell'evento da un'origine specifica. Sentinel 5 supporta principalmente le connessioni remote “senza servizio di raccolta” alle origini. I servizi di raccolta possono tuttavia essere distribuiti su dispositivi specifici dove un approccio remoto è meno efficiente.

I servizi di raccolta sono controllati da Sentinel Control Center, che regola le comunicazioni tra i Servizi di raccolta e la piattaforma di Sentinel per l'analisi in tempo reale, l'elaborazione della correlazione e la risposta ai casi.

Motore e Gestione servizi di raccolta

Gestione servizio di raccolta gestisce i Servizi di raccolta, monitora i messaggi di stato del sistema ed applica i filtri agli eventi in base alle richieste. Le funzioni principali di Gestione servizio di raccolta comprendono la trasformazione degli eventi, l'aggiunta di rilevanza aziendale agli eventi mediante tassonomia, l'applicazioni di filtri globali sugli eventi, l'instradamento degli eventi e l'invio di messaggi di stato al server Sentinel.

Un motore del servizio di raccolta è il componente di interpretazione che analizza il codice del Servizio di raccolta.

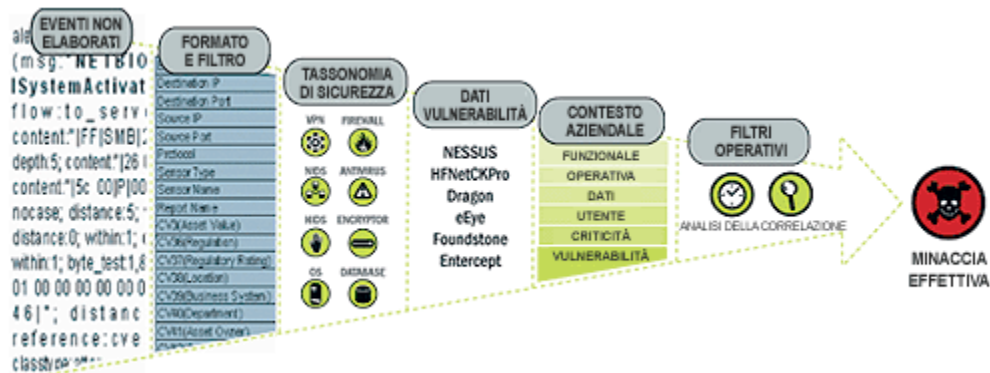
Generatore servizi di raccolta

Il Generatore servizi di raccolta è un’applicazione autonoma utilizzata per creare, configurare ed eseguire il debug dei servizi di raccolta. Questa applicazione viene utilizzata come ambiente di sviluppo integrato (o IDE) che consente all'utente di creare nuovi servizi di raccolta per analizzare i dati prodotti dai dispositivi di origine mediante un linguaggio interpretativo avente scopo specifico realizzato per gestire la natura della rete e gli eventi di sicurezza.

Servizi comuni

Tutti i componenti sopra descritti relativi a questo strato di raccolta e arricchimento si basano su una serie di servizi comuni. Questi servizi di utility costituiscono il tessuto della raccolta e dell'arricchimento dei dati e aiutano a filtrare le informazioni (mediante filtri globali), applicando tag definiti dall'utente per arricchire le informazioni sugli eventi (mediante la rilevanza aziendale e i servizi di mappatura tassonomici) e regolando le funzioni dei servizi di raccolta dei dati (mediante servizi di controllo e di comando).

Tassonomia: quasi tutti i prodotti di sicurezza producono eventi in formati differenti e con contenuto variabile. Ad esempio, Windows e Solaris segnalano in modo differente un errore di login.

La tassonomia di Sentinel traduce in modo automatico i dati dei prodotti eterogenei in termini significativi, consentendo una visione omogenea in tempo reale della sicurezza dell'intera rete. La tassonomia di Sentinel formatta e filtra gli eventi di sicurezza non elaborati prima di aggiungere il contesto dell'evento al flusso di dati. Questo processo formatta tutti i dati di sicurezza nella struttura più ottimale ai fini dell'elaborazione da parte del motore di correlazione di Sentinel, come illustrato nel diagramma seguente.

Rilevanza aziendale: Sentinel 5 inserisce i dati contestuali di rilevanza aziendale direttamente nel flusso degli eventi. Sono compresi 135 campi personalizzabili dove gli utenti possono aggiungere informazioni specifiche sulle risorse, ad esempio unità commerciale, proprietario, valore della risorsa, geografia. Dopo aver aggiunto tali informazioni al sistema, tutti gli altri componenti possono sfruttare il contesto aggiuntivo.

Rilevamento degli exploit: il rilevamento degli exploit consente la notifica immediata e processabile degli attacchi ai sistemi vulnerabili. Fornisce un collegamento in tempo reale tra le firme IDS e i risultati di scansione delle vulnerabilità, inviando una notifica automatica e immediata agli utenti di un tentativo di attacco rivolto a sfruttare un sistema vulnerabile. Ciò consente di migliorare incredibilmente l'efficienza e l'efficacia dell'azione di risposta.

Il rilevamento degli exploit fornisce agli utenti aggiornamenti delle mappature tra IDS e le firme dei prodotti di scansione delle vulnerabilità. Le mappature comprendono un elenco esaustivo di IDS e delle scansioni delle vulnerabilità. Gli utenti devono semplicemente caricare i risultati delle scansioni delle vulnerabilità in Sentinel. Il rilevamento degli exploit li analizza in modo automatico e aggiorna gli appositi Servizi di raccolta IDS. Utilizza le conoscenze integrate dello stato delle vulnerabilità per assegnare in modo efficace ed efficiente le priorità delle risposte alle minacce di sicurezza in tempo reale.

Quando viene lanciato un attacco contro una risorsa vulnerabile, il rilevamento degli exploit avvisa gli utenti notificando il corrispondente livello di gravità della vulnerabilità sfruttata. Gli utenti possono quindi intraprendere azioni immeditate sugli eventi classificati ad alta priorità. Questo sistema si basa sul monitoraggio degli avvisi e migliora l'efficacia della risposta ai casi focalizzando la reazione sugli attacchi noti contro le risorse vulnerabili.

Il rilevamento degli exploit consente inoltre agli utenti di mappare o “non mappare” le firme e le vulnerabilità in modo da sincronizzare i falsi positivi e i falsi negativi e di sfruttare le firme personalizzate o le scansioni delle vulnerabilità.

Strato logico aziendale

Il kernel della piattaforma di Sentinel 5 è costituito da una serie di servizi loosely-coupled che possono essere eseguiti in una configurazione autonoma o in una topologia distribuita. Questa architettura orientata verso il servizio (SOA) è chiamata iSCALE. In specifico, il SOA di Sentinel comprende una serie di motori, servizi e API che collaborano per scalare in modo lineare la soluzione rispetto a un aumento del carico di dati e/o del carico di lavoro di elaborazione.

I servizi di Sentinel sono eseguiti in container specializzati e consentono di elaborare e scalare senza precedenti in quanto sono ottimizzati per il trasporto e l'elaborazione in base ai messaggi. I servizi principali che costituiscono il server Sentinel comprendono:

- Servizio remoto
- Servizio DAS (Data Access Service)
- Servizio di gestione delle interrogazioni
- Servizio di correlazione
- Servizio Workflow
- Visualizzazione eventi
- Risposta ai casi
- Rapporti
- Advisor
- Stato
- Amministrazione

Servizio remoto

Il Servizio remoto di Sentinel 5 è il meccanismo mediante il quale i programmi del server e del client comunicano. In genere questo meccanismo viene indicato come un'applicazione oggetti distribuita.

In specifico, il Servizio remoto offre le seguenti funzioni:

- Individua gli oggetti remoti: grazie ai metadati che descrivono il nome dell'oggetto o il token di registrazione, anche se non è richiesta la posizione effettiva, poiché il bus messaggi iSCALE consente la trasparenza della posizione.
- Comunica con gli oggetti remoti: i dettagli delle comunicazioni tra oggetti remoti sono gestiti dal bus messaggi iSCALE.
- Esegue lo streaming e della ripartizione degli oggetti: quando una grande quantità di dati deve essere trasferita dal client al server e viceversa, questi oggetti sono ottimizzati per il caricamento dei dati su richiesta.
- Esegue le richiamate: un altro schema e strato di astrazione integrato nel Servizio remoto che consente la comunicazione degli oggetti remoti PTP.
- Monitora il servizio e le statistiche: fornisce statistiche sulle prestazioni e sul carico per l'utilizzo dei servizi remoti.

Servizio DAS (Data Access Service)

Il servizio DAS (Data Access Service) è un servizio di gestione degli oggetti che consente agli utenti di definire gli oggetti utilizzando i metadati. Il servizio DAS gestisce l'oggetto e l'accesso agli oggetti e automatizza la trasmissione e la persistenza. DAS viene inoltre utilizzato come facciata per accedere ai dati da qualsiasi archivio di dati persistente, ad esempio i servizi di directory o i file. Le operazioni di DAS comprendono l'accesso uniforme ai dati mediante JDBC e strategie opzionali di inserimento degli eventi a elevate prestazioni mediante l'utilizzo di connettori nativi (ad esempio, OCI per Oracle 9i e ADO per Microsoft SQL Server).

Servizio di gestione delle interrogazioni

Il servizio di gestione delle interrogazioni regola le richieste di cronologia degli eventi e di drill-down da Sentinel Control Center. Questo servizio è un componente integrale per l'implementazione dell'algoritmo di paging utilizzato nella capacità di ricerca di Cronologia degli eventi. Converte i filtri definiti dall'utente in criteri validi e vi allega criteri di sicurezza prima che gli eventi siano recuperati. Questo servizio garantisce inoltre che i criteri non vengano modificati durante una transazione della cronologia degli eventi sottoposta a paging.

Servizio di correlazione

L'algoritmo di correlazione di Sentinel 5 calcola gli eventi correlati analizzando il flusso di dati in tempo reale. Pubblica gli eventi correlati in base alle regole definite dall'utente prima che l'evento arrivi sul database. Le regole nel motore di correlazione possono rilevare uno schema in un singolo evento di una finestra di esecuzione di eventi. Quando viene rilevata una correlazione, il motore di correlazione genera un evento correlato descrivendo lo schema individuato e può creare un caso o attivare un workflow di risposta mediante iTRAC. Il motore di correlazione funziona con un componente del processo di verifica delle regole che elabora le espressioni della regola di correlazione e convalida la sintassi dei filtri. Oltre a fornire una serie esaustiva di regole di correlazione, il motore di correlazione di Sentinel offre vantaggi specifici rispetto ai motori di correlazione centrati sui database.

- Basandosi su un'elaborazione in memoria anziché su inserimenti e letture del database, il motore di correlazione viene eseguito, durante volumi elevati nello stato stazionario e durante picchi di eventi quando sottoposto ad attacchi, all'ora in cui le prestazioni di correlazione sono più critiche.
- I volumi di correlazione non rallentano altri componenti del sistema. Pertanto, l'interfaccia utente rimane reattiva, soprattutto con volumi elevati di eventi.
- Correlazione distribuita: le organizzazioni possono distribuire motori di correlazione multipli, ognuno sul proprio server, senza la necessità di replicare le configurazioni o aggiungere database. La possibilità di scalare i componenti in modo indipendente garantisce una scalabilità e prestazioni efficaci in termini di costo.
- Il motore di correlazione può aggiungere eventi ai casi dopo che sono stati determinati.

Agli utenti viene consigliato di utilizzare un parametro di misurazione chiamato ERPS (Event Rules per Second). ERPS è la misura del numero di eventi che possono essere esaminati da una regola di correlazione al secondo. Questa misurazione è un ottimo indicatore delle prestazioni in quanto valuta l'impatto sulle prestazioni quando due fattori si intersecano: Eventi al secondo e numero di regole in uso.

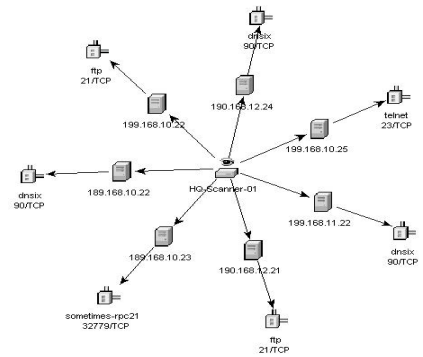
Servizio Workflow (iTRAC)

Il Servizio workflow riceve le attivazioni sulla creazione dei casi e avvia i processi di workflow in base ai modelli di workflow predefiniti. Gestisce il ciclo di vita di questi processi generando gli elementi di lavoro oppure eseguendo attività. Questo servizio conserva inoltre una cronologia dei processi completati che possono essere utilizzati per la verifica delle risposte ai casi.

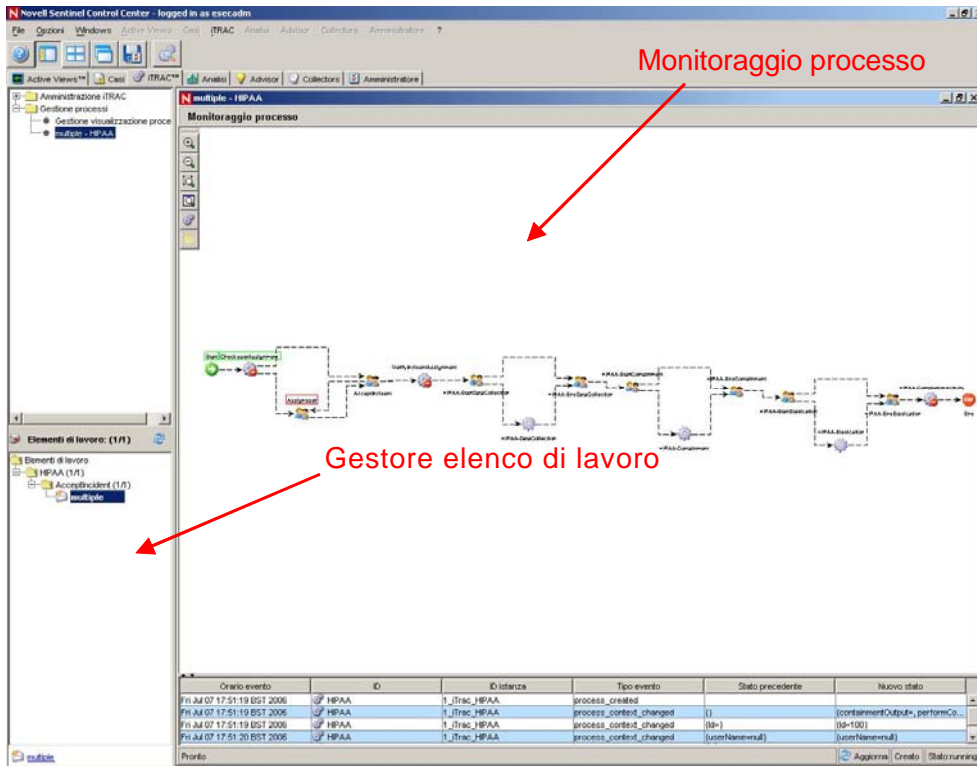
Visualizzazione eventi

Active Views™, l'interfaccia utente grafica interattiva per la visualizzazione degli eventi, fornisce un dashboard integrato per la gestione della sicurezza con una serie esaustiva di strumenti di visualizzazione e analisi in tempo reale per facilitare il rilevamento e l'analisi delle minacce. Gli utenti possono monitorare gli eventi in tempo reale ed eseguire drill-down immediati compresi tra secondi e ore degli eventi passati. Un'ampia gamma di strumenti e

diagrammi di visualizzazione consente di eseguire il monitoraggio delle informazioni mediante rappresentazioni grafiche a barre 3D, in pila 2D, a linee o a nastri e molto altro ancora. Dalla dashboard di Active Views è possibile visualizzare ulteriori informazioni di rilievo, compresa la notifica degli exploit delle risorse (rilevamento degli exploit), la visualizzazione delle informazioni sulle risorse e le associazioni grafiche tra IP di origine e IP di destinazione pertinenti.

Poiché Active Views utilizza l'architettura iSCALE, gli analisti possono eseguire drill-down rapidi per ulteriore analisi in quanto Active Views garantisce l'accesso diretto ai dati sugli eventi residenti in memoria in tempo reale, il che consente di gestire in modo semplice migliaia di eventi al secondo senza alcuna ripercussione sulle prestazioni. I dati sono conservati nella memoria e scritti sul database in base alle esigenze (in Active Views è possibile memorizzare fino a 8 ore di dati in memoria con carichi di eventi tipici). Questa visualizzazione continua, in tempo reale e orientata sulle prestazioni è fondamentale in caso di attacco o nello stato stazionario.

Risposta ai casi tramite iTRAC

iTRAC trasforma la tradizionale gestione delle informazioni di sicurezza da un ruolo passivo di “invio avvisi e visualizzazione” in un ruolo di “risposta ai casi praticabile” consentendo alle organizzazioni di definire e documentare i processi di risoluzione dei casi e guidare, implementare e tenere traccia dei processi di risoluzione quando un caso o una violazione sono stati rilevati.

Sentinel 5 viene fornito con modelli di processi “pronti per l'utilizzo” che utilizzano le linee guida del SANS Institute per la gestione dei casi. Gli utenti possono iniziare da questi processi predefiniti e configurare attività specifiche per riflettere le pratiche migliori della propria organizzazione. I processi iTRAC possono essere attivati automaticamente dalla creazione di casi o dalle regole di correlazione, oppure essere attivati manualmente da un esperto di sicurezza o di revisione autorizzato. iTRAC conserva un giornale di controllo di tutte le azioni allo scopo di supportare la conformità con la generazione di rapporti e le analisi cronologiche.

In un elenco di lavoro sono segnalate all'utente tutte le attività che sono state a lui assegnate e un monitoraggio del processo garantisce la visibilità in tempo reale dello stato di un processo nel corso del ciclo di vita del processo di risoluzione.

Il framework dell'attività di iTRAC consente agli utenti di personalizzare le attività automatizzate o manuali per processi specifici di risoluzione dei casi. I modelli del processo iTRAC possono essere configurati utilizzando il framework delle attività allo scopo di trovare una corrispondenza tra il modello e le migliori pratiche di un'organizzazione. Le attività sono eseguite direttamente da Sentinel Control Center.

Il framework di automazione di iTRAC utilizza due componenti principali: il container delle attività e il container del workflow. Il primo automatizza l'esecuzione delle attività per la serie specifica di passaggi in base alle regole di input, mentre il secondo automatizza l'esecuzione del workflow in base alle attività mediante un elenco di lavoro. Le regole di input si basano sullo standard XPDL (XML Processing Description Language) e offrono un modello formale per l'espressione dei processi eseguibili in un'azienda. Questo approccio basato su standard per l'implementazione di specifiche regole e gruppi di regole business garantisce agli utenti la possibilità di definire i processi nel futuro.

Servizio di generazione dei rapporti

Il servizio di generazione dei rapporti consente la generazione di rapporti, compresi i rapporti cronologici e sulle vulnerabilità. Sentinel 5 offre rapporti pronti all'uso e consente agli utenti di configurare rapporti personalizzati mediante Crystal Reports. Alcuni esempi di rapporti integrati in Sentinel 5:

- Analisi delle tendenze
- Stato di sicurezza delle linee di risorse aziendali o critiche

- Tipi di attacco
- Risorse interessate
- Tempi di risposta e risoluzione
- Violazioni di conformità ai criteri

Advisor

Sentinel Advisor è un modulo opzionale che collega i dati degli avvisi in tempo reale di Sentinel alle informazioni sulle vulnerabilità e i rimedi noti, colmando il divario tra il rilevamento dei casi e la relativa risposta. Advisor consente alle organizzazioni di determinare se gli eventi sfruttano vulnerabilità specifiche e l'impatto sulle risorse causato da tali attacchi. In Advisor sono inoltre contenute informazioni sulle vulnerabilità che gli attacchi intendono sfruttare, i potenziali effetti degli attacchi, se eseguiti con successo e le necessarie azioni da intraprendere per la risoluzione. Le procedure di risoluzione consigliate vengono implementate e monitorate mediante i processi di risposta ai casi di iTRAC.

Stato

Il servizio relativo allo stato consente agli utenti di ottenere una visualizzazione completa della piattaforma distribuita Sentinel 5. Aggrega informazioni sullo stato prodotte da vari processi che sono generalmente distribuiti su vari server. Le informazioni sullo stato sono visualizzate periodicamente in Sentinel Control Center per l'utente finale.

Amministrazione

La struttura amministrativa consente la gestione degli utenti e le strutture di definizione delle impostazioni che sono generalmente richieste dagli amministratori delle applicazioni di Sentinel 5.

Servizi comuni

Tutti i componenti sopra descritti relativi a questo strato logico aziendale dell'architettura si basano su una serie di servizi comuni. Questi servizi di utility aiutano ad applicare un filtro accurato (mediante il motore filtri) degli eventi agli utenti, il monitoraggio costante delle statistiche sullo stato del sistema (mediante il monitoraggio di stato) e gli aggiornamenti dinamici dei dati a livello di sistema (mediante il Servizio di mappatura). Questi servizi di utility costituiscono congiuntamente il tessuto dei servizi loosely-coupled che consentono di elaborare e scalare in modo incredibile rispetto al trasporto in base al bus messaggi ai fini dell'analisi e dell'elaborazione in tempo reale.

Strato di presentazione

Al livello di presentazione viene eseguito il rendering dell'interfaccia dell'applicazione per l'utente finale. Il Sentinel Command Center è un dashboard esaustivo che presenta le informazioni all'utente.

Moduli del prodotto

Sentinel Control Center

Sentinel Control Center è un dashboard integrato e potente di gestione della sicurezza. Le visualizzazioni intuitive consentono agli analisti di identificare velocemente le nuove

tendenze o i nuovi attacchi, di elaborare e interagire con le informazioni grafiche in tempo reale e di rispondere ai casi. Le funzioni principali comprendono:

- Active Views: analisi e visualizzazione in tempo reale
- Casi: creazione e gestione dei casi
- Analisi: definizione e gestione delle regole di correlazione
- iTRAC: gestione dei processi per la documentazione, l'applicazione e il controllo dei processi di risoluzione dei casi.
- Generazione rapporti: cronologia dei rapporti e delle misurazioni

Sentinel Wizard

Sentinel Wizard raccoglie dati dai dispositivi di origine e restituisce un flusso di eventi più ricco inserendo tassonomia, il rilevamento degli exploit e la rilevanza aziendale nel flusso di dati prima che gli eventi siano correlati, analizzati e inviati al database. Un flusso di eventi più corposo indica che i dati vengono collegati al contesto aziendale necessario per identificare e riparare alle minacce interne o esterne e alle violazioni alle norme. Tutte le configurazioni dovrebbero includere una o più procedure guidate per fornire ai clienti la possibilità di distribuire i componenti del prodotto nella propria infrastruttura in base alla topologia della rete in uso.

Sentinel Advisor

Sentinel Advisor è un modulo opzionale che collega i dati degli avvisi in tempo reale di Sentinel alle informazioni sulle vulnerabilità e i rimedi noti.

Sommario

Questa guida contiene i capitoli seguenti:

- Capitolo 1: Introduzione a Sentinel
- Capitolo 2: Esplorazione di Sentinel Control Center
- Capitolo 3: Scheda Active Views™
- Capitolo 4: Scheda Casi
- Capitolo 5: Scheda iTRAC™
- Capitolo 6: Scheda Analisi
- Capitolo 7: Scheda Advisor
- Capitolo 8: Scheda Servizi di raccolta
- Capitolo 9: Scheda Amministratore
- Capitolo 10: Gestione dati Sentinel
- Capitolo 11: Utility
- Capitolo 12: Riferimento rapido
- Appendice A: Eventi di sistema

Convenzioni utilizzate

Note e avvertenze

NOTA: Le Note forniscono ulteriori informazioni che possono rivelarsi utili.

ATTENZIONE: Le avvertenze forniscono ulteriori informazioni che possono essere utili per evitare danni al sistema o perdite di dati.

Comandi

I comandi sono visualizzati con il font courier. Ad esempio:

```
useradd -g dba -d /export/home/oracle -m -s /bin/csh
   oracle
```

Altri riferimenti Novell

Sono disponibili i manuali seguenti con i CD di installazione di Sentinel.

- Guida all'installazione di Sentinel™ 5
- Guida dell'utente di Sentinel™
- Guida dell'utente di Sentinel™ 5 Wizard
- Guida di riferimento dell'utente di Sentinel™ 5
- Guida all'integrazione con soluzioni di terze parti di Sentinel™5
- Note di rilascio

Come contattare Novell

- Sito Web: http://www.novell.com
- Supporto tecnico Novell: http://www.novell.com/support/index.html
- Per supporto 24x7, 800-858-4000

2 Esplorazione di Sentinel Control Center

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Sentinel Control Center è composto da:

- Barra dei menu
- Barra degli strumenti
- Schede

In questo capitolo vengono inoltre trattati gli argomenti seguenti:

- Avvio di Sentinel Control Center
- Modifica dell’interfaccia di Sentinel Control Center
- Salvataggio delle preferenze utente
- Modifica della password di Sentinel

Avvio di Sentinel Control Center

Avvio di Sentinel Control Center in Windows

Avvio di Sentinel Control Center in Windows

1. *Fare clic su Start > Sentinel > Sentinel Control Center oppure fare clic sull'icona di Sentinel Control Center sul desktop*.
2. Immettere il nome utente e la password, quindi fare clic su *OK*.

Avvio di Sentinel Control Center in UNIX

Avvio di Sentinel Control Center in UNIX

1. In qualità di utente esecadm, passare alla directory:

   ```
   $ESEC_HOME/sentinel/console
   ```

2. Eseguire il comando seguente:

   ```
   ./run.sh
   ```

3. Immettere il nome utente e la password, quindi fare clic su *OK*.

Barra dei menu

Sotto la barra del titolo ci sono dieci menu. Dall'angolo superiore sinistro all'angolo superiore destro sono disponibili i menu File, Opzioni, Finestre, Active Views, Casi, iTRAC, Advisor, Servizi di raccolta, Amministratore e ?.

I menu File, Opzioni, Finestre e ? sono sempre disponibili. La presenza di altre opzioni dipende dalle schede attive e dalle autorizzazioni di cui si dispone.

Menu File

- Salva preferenze
- Esci

Menu Opzioni

- Cambia password...
- Disposizione schede
  - In alto
  - In basso
- Aggancia barra di spostamento
- Mostra barra di spostamento

Menu Finestre

- Sovrapponi tutte
- Affianca tutte
  - Affianca e adatta
  - Affianca orizzontalmente
  - Affianca verticalmente
- Riduci a icona tutte

- Ripristina tutte
- Chiudi tutte

Active Views™

- Proprietà
- Crea visualizzazione Active Views
- Interrogazione eventi
- Tempo reale evento
  - Istantanea
  - Gestisci colonne

Casi

- Visualizza Gestione visualizzazione caso
- Crea caso
- Configurazione visualizzatori per allegati

iTRAC™

- Visualizza Gestione processi

Analisi

- Crea rapporto

Advisor

- Crea rapporto

Servizi di raccolta

- Mostra Gestione visualizzazione servizi di raccolta

Amministratore

- Configurazione rapporti
- Regole di correlazione
- Gestione motore di correlazione
- Configurazione filtri globali
- Configurazione menu
- Configurazione filtri
- Configurazione utente

?

- ?
- Informazioni su Sentinel

Barra degli strumenti

Nella barra degli strumenti sono sempre visualizzati cinque pulsanti. La visualizzazione di altri pulsanti dipende dalle schede o dalle finestre attive e dalle autorizzazioni utente di cui si dispone.

Barra degli strumenti di sistema

I cinque pulsanti di sistema visualizzati nella barra degli strumenti sono:

- Visualizza Guida di Sentinel
- Mostra/Nascondi finestra di spostamento
- Affianca tutte le finestre visualizzate
- Sovrapponi tutte le finestre visualizzate
- Salva preferenze utente

Scheda Active Views™

Quando la scheda ActiveViews™ è attiva, sono disponibili i pulsanti seguenti.

- Visualizzazioni Active Views
- Avvia interrogazione eventi

Finestra Numero eventi nel tempo

Quando la finestra Numero eventi nel tempo è attiva, sono disponibili i pulsanti seguenti.

- Istantanea tabella Numero eventi nel tempo
- Gestisci colonne di tabella tempo reale eventi

Grafico Numero eventi nel tempo

Quando il grafico Numero eventi nel tempo è attivo, all'interno sono disponibili i pulsanti seguenti.

- Blocca/Sblocca grafico
- Aumenta intervallo di visualizzazione
- Riduci intervallo di visualizzazione
- Aumenta tempo di visualizzazione
- Riduci tempo di visualizzazione

Quando si fa clic sul pulsante Blocca grafico, i pulsanti disponibili sono:

- Blocca/Sblocca grafico
- Aumenta intervallo di visualizzazione
- Riduci intervallo di visualizzazione
- Aumenta tempo di visualizzazione
- Riduci tempo di visualizzazione
- Ingrandisci

- Riduci
- Esegui drill-down su evento
- Salva come file html

Finestra Istantanea

Quando la finestra Istantanea è attiva, è disponibile il pulsante seguente.

- Gestisci colonne

Scheda Casi

Quando la scheda Casi è attiva, sono disponibili i pulsanti seguenti.

- Visualizza Gestione visualizzazione caso
- Crea un nuovo caso
- Configura visualizzatori di allegati

Caso

Quando si apre un caso, è disponibile il pulsante seguente.

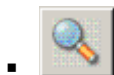
- Gestisci colonne di eventi associati

iTRAC

Quando la scheda iTRAC è attiva, è disponibile il pulsante seguente.

- Visualizza Gestione visualizzazione processi

Schede Analisi e Advisor

Quando la scheda Analisi o Advisor è attiva, è disponibile il pulsante seguente.

- Crea rapporto

Scheda Servizi di raccolta

Quando la scheda Servizi di raccolta è attiva, sono disponibili i pulsanti seguenti.

- Mostra Gestione visualizzazione Gestione servizi di raccolta
- Mostra Gestione visualizzazione servizi di raccolta

Scheda Amministratore

Quando la scheda Amministratore è attiva, sono disponibili i pulsanti seguenti.

- Visualizza Configurazione rapporti
- Visualizza Regole di correlazione
- Visualizza Gestione motore di correlazione
- Visualizza Configurazione filtri globali
- Visualizza Configurazione menu
- Visualizza Gestione filtri
- Visualizza Gestione utenti
- Gestione visualizzazioni server

Finestra Gestione filtri

Quando la finestra Gestione filtri è attiva, sono disponibili i pulsanti seguenti.

- Crea un nuovo filtro
- Elimina il filtro selezionato (attivo quando è selezionato un filtro)

Finestra Configurazione menu

Quando la finestra Configurazione menu è attiva e in modalità di modifica, sono disponibili i pulsanti seguenti.

- Crea nuova voce di menu
- Elimina voce di menu
- Attiva voce di menu
- Disattiva voce di menu

Schede

A seconda delle autorizzazioni utente di cui si dispone, in Sentinel Control Center sono visualizzate le schede di seguito elencate. Per visualizzarle, è necessario disporre delle autorizzazioni appropriate.

- Active Views™
- Casi
- iTRAC™
- Analisi
- Advisor
- Servizi di raccolta
- Amministratore

Per ulteriori informazioni sulle schede, consultare i capitoli relativi a ognuna di esse.

Modifica dell'interfaccia di Sentinel Control Center

È possibile modificare l'interfaccia di Sentinel Control Center eseguendo le operazioni seguenti:

- Impostazione della posizione delle schede
- Visualizzazione della barra di spostamento
- Agganciamento e sblocco della barra di spostamento
- Sovrapposizione di finestre
- Affiancamento di finestre
- Riduzione a icona e ripristino di tutte le finestre
- Chiusura simultanea di tutte le finestre

Impostazione della posizione delle schede

Per impostare la posizione delle schede

1. Fare clic su *Opzioni > Disposizione schede*.
2. Selezionare l'opzione In alto o In basso.

Visualizzazione della barra di spostamento

Per visualizzare o nascondere la barra di spostamento

1. Fare clic su *Opzioni > Mostra barra di spostamento* (attiva o disattiva).

Agganciamento e sblocco della barra di spostamento

Per agganciare o sbloccare la barra di spostamento

1. Fare clic su *Opzioni > Aggancia barra di spostamento* (attiva o disattiva).

Sovrapposizione di finestre

Per sovrapporre le finestre

1. Fare clic su *Finestre > Sovrapponi tutte.* Tutte le finestre aperte nel riquadro destro verranno sovrapposte.

Affiancamento di finestre

Per affiancare le finestre

1. *Fare clic su Finestre > Affianca tutte.*
2. Selezionare a scelta:
   - Affianca e adatta
   - Affianca verticalmente
   - Affianca orizzontalmente

Riduzione a icona e ripristino di tutte le finestre

Per ridurre a icona tutte le finestre

1. Fare clic su *Finestre* > *Riduci a icona tutte. Tutte le finestre aperte nel riquadro destro saranno ridotte a icona*.

Per ripristinare le dimensioni originali di tutte le finestre

Per ripristinare le dimensioni originali di tutte le finestre

1. Fare clic su *Finestre* > *Ripristina tutte.* Saranno ripristinate le dimensioni originali di tutte le finestre aperte nel riquadro destro.

Per ripristinare una singola finestra

Per ripristinare le dimensioni originali di una singola finestra

1. Fare clic *sulla finestra ridotta a icona.* La finestra sarà visualizzata nelle dimensioni originali.

Chiusura simultanea di tutte le finestre

Per chiudere tutte le finestre contemporaneamente

1. Fare clic su *Finestre* > *Chiudi tutte.*

Salvataggio delle preferenze utente

È necessario disporre dell'autorizzazione utente per il salvataggio dell'area di lavoro.

Le preferenze che è possibile salvare sono:

- Finestre permanenti, ovvero quelle che possono essere ricreate perché non dipendono dai dati disponibili al momento della creazione originale. Le finestre di riepilogo e Active Views, ad esempio, possono essere salvate. Le finestre temporanee, come le istantanee e le interrogazioni rapide, invece, non possono essere salvate. Tutte le finestre elencate nella barra di spostamento dell'amministratore vengono salvate; nessuna finestra secondaria aperta facendo doppio clic su un'opzione contenuta al suo interno, invece, può essere salvata.
- Posizioni delle finestre
- Dimensioni delle finestre, inclusa la finestra dell'applicazione.
- Posizioni delle schede
- Barra di spostamento agganciata o sbloccata, visualizzata o nascosta.

Per salvare le preferenze

1. Fare clic su *File, quindi scegliere Salva preferenze oppure* fare clic sul pulsante *Salva preferenze.*

Modifica della password di Sentinel Control Center

NOTA: Per soddisfare le rigorose configurazioni di sicurezza necessarie per la certificazione dei criteri comuni, Novell richiede una password che abbia le caratteristiche seguenti:

1. Scegliere password costituite da un minimo di 8 caratteri, di cui almeno uno MAIUSCOLO, uno minuscolo, uno speciale (!@#$%^&*()_+) e uno numerico (0-9).

2. Non è possibile includere nella password l'indirizzo di e-mail o una parte qualsiasi del nome completo.

3. La password non deve essere una parola “comune”, ovvero una parola inclusa nel dizionario o di uso gergale.

4. È necessario che nella password non siano incluse parole di alcuna lingua poiché esistono numerosi programmi per la violazione delle password in grado di elaborare milioni di possibili combinazioni di parole in pochi secondi.

5. È consigliabile scegliere una password facile da ricordare e allo stesso tempo complessa. Ad esempio, Mfhq5#ao (Mio Figlio Ha Quasi 5 Anni Ormai) oppure VaNdq#3a (Vivo a Napoli Da Quasi 3 anni).

Per modificare la password di Sentinel Control Center

1. Fare clic su *Opzioni, quindi scegliere Cambia password*.
2. Immettere la password da cambiare.
3. Immettere la nuova password e specificarla di nuovo per la verifica.

NOTA: La procedura consigliata prevede l'utilizzo di password composte da almeno 8 caratteri alfanumerici.

4. Fare clic su *OK*.

3 Scheda Active Views™

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Per utilizzare la scheda Active Views™ è necessario disporre dell'autorizzazione appropriata. Se questa autorizzazione non viene assegnata, nessuna delle autorizzazioni relative alle azioni eseguibili con questa scheda sarà disponibile.

Nella scheda Active Views è possibile monitorare, quasi in tempo reale, gli eventi nel momento in cui si verificano ed eseguire interrogazioni su questi eventi. Il monitoraggio degli eventi può essere eseguito in una tabella oppure attraverso una rappresentazione con grafico a barre 3D, in pila 2D, a linee o a nastri.

Scheda Active Views: Descrizione

Le visualizzazioni degli eventi sono formattate come tabelle. La configurazione della scheda Active Views è determinata dal file das_rt.xml. I due tipi di visualizzazioni Active Views sono una tabella eventi in tempo quasi reale con rappresentazione grafica e di tipo Istantanea.

- Tabella eventi in tempo quasi reale
  - Conserva fino a 750 eventi ogni 30 secondi.
  - Per default, nel client sono archiviati gli eventi memorizzati nella cache relativi a un periodo di 24 ore. È possibile configurare questo valore mediante Proprietà visualizzazione Active Views.
  - Per default, nella tabella eventi sono visualizzati al massimo 30.000 eventi. È possibile configurare questo valore mediante Proprietà visualizzazione Active Views.
  - Per default, la tabella eventi viene aggiornata ogni 30 secondi (ritardo tempo di invio). L'aggiornamento viene rappresentato mediante una linea grigia nella tabella eventi.

3	2005.06.21 / 06:34:38 EDT			Threshold_e›
2	2005.06.21 / 06:34:38 EDT	206.158.21.6	192.168.10.1	Password_ex
2	2005.06.21 / 06:34:28 EDT	190.168.12.21	190.168.12.21	Program_exe

Negli eventi in cui sono presenti più di 750 eventi in un intervallo di 30 secondi, verrà visualizzata una linea di separazione rossa per indicare che è presente un numero maggiore di eventi rispetto a quelli visualizzati.

3	2005.06.21 / 07:07:00 EDT	172.16.112.50	172.16.0.65	unsuccessfu
3	2005.06.21 / 07:07:00 EDT	172.16.112.50	172.16.0.65	suspicious-fil
3	2005.06.21 / 07:06:58 EDT	172.16.112.50	172.16.0.65	successful-a

  - Dopo aver salvato le preferenze dell'utente, la raccolta dei dati proseguirà per 4 giorni. Ad esempio, se si salvano le preferenze, si esegue la disconnessione e si esegue nuovamente la connessione il giorno seguente, nella visualizzazione Active Views i dati saranno visualizzati come se non la disconnessione non fosse mai stata eseguita.
  - Se viene creata e non salvata, la visualizzazione Active Views continuerà a raccogliere dati per un'ora. Se nello stesso intervallo di tempo viene creata una visualizzazione Active Views identica, verranno visualizzati i dati relativi all'ultima ora.
- Istantanea: visualizzazioni di una tabella Visualizzazione tempo reale eventi con indicazione dell'ora.

Le caratteristiche seguenti rendono univoca una visualizzazione Active Views.

- Filtro assegnato a una visualizzazione Active Views
- Attributo dell'asse z
- Filtro di sicurezza assegnato a un utente

La scheda Active Views consente di:

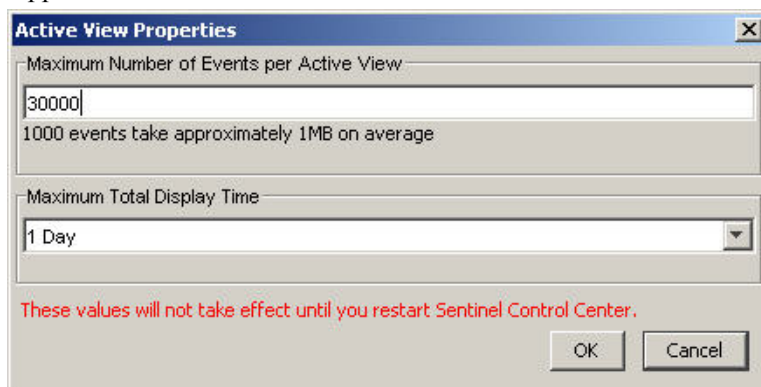
- Riconfigurare Active Views
- Aggiungere Eventi a un caso
- Chiudere un'Istantanea o una finestra di navigazione visiva
- Creare un caso
- Personalizzare le opzioni del menu con Eventi
- Eliminare un'Istantanea o una finestra di navigazione visiva
- Interrogazione eventi
- Mappa grafica
- Visualizzare i dati Advisor
- Gestire le colonne
- Inviare messaggi relativi agli eventi via e-mail
- Mostrare o nascondere i dettagli degli eventi
- Creare un'Istantanea di una finestra di navigazione visiva
- Visualizzare gli eventi che attivano un evento correlato
- Visualizzare la visualizzazione delle vulnerabilità
- Visualizzare dati di risorse
- Eseguire operazioni HP – OpenView e Service Desk
- Eseguire operazioni Remedy

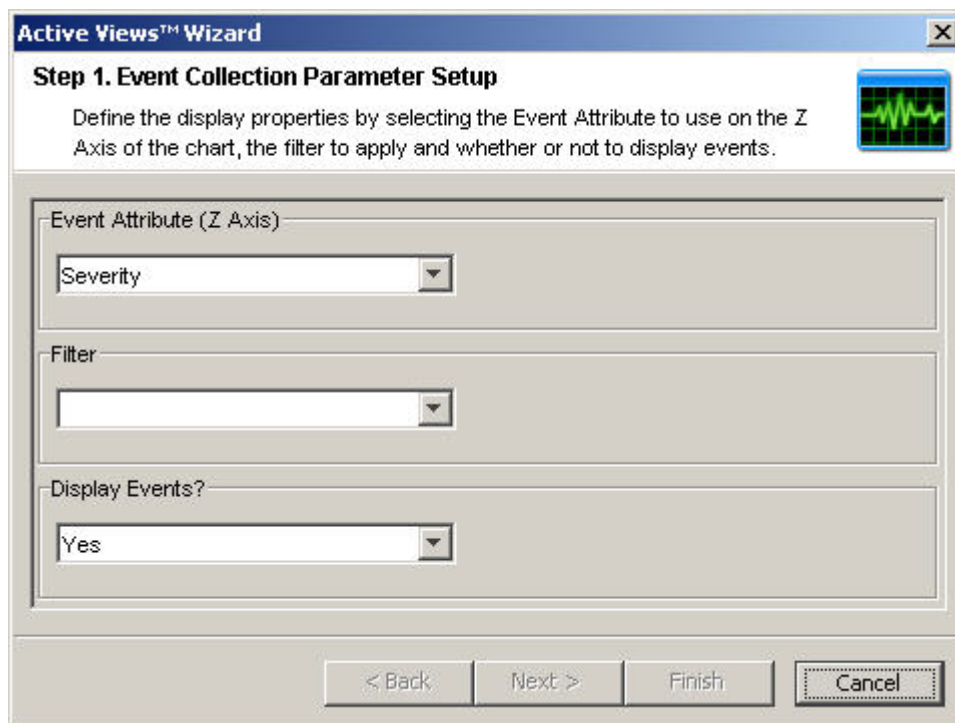
In qualità di utente, è possibile modificare i valori (nomi delle colonne) in modo da visualizzare i nomi logici e compilarli in tutto il sistema. È possibile applicare attributi al flusso di eventi rilevante per la propria azienda. Per ulteriori informazioni, vedere il capitolo 10 relativo a Gestione dati Sentinel, la Guida dell'utente di Wizard e la Guida di riferimento dell'utente di Sentinel.

Riconfigurazione degli eventi massimi in Active Views e del valore memorizzato nella cache

Le Proprietà visualizzazione Active Views consentono di configurare il numero massimo di eventi che è possibile visualizzare in Active Views e il tempo di memorizzazione nella cache in ogni client. Il numero totale massimo di default degli eventi in Active Views è 30.000 eventi. Il valore temporale di default per la memorizzazione nella cache in Active Views è 24 ore.

Per riconfigurare gli Eventi massimi di Active Views e il Valore memorizzato nella cache

1. Fare clic sulla scheda *Active Views*.
2. Fare clic su *Active Views* > *Proprietà.*
3. Apportare le modifiche desiderate.

I nuovi valori avranno effetto solo dopo aver riavviato Sentinel Control Center.

Per visualizzare gli eventi in tempo reale

Per visualizzare gli eventi in tempo reale

1. Fare clic sulla scheda *Active Views*.
2. Fare clic su *Active Views* > *Crea visualizzazione Active Views* oppure fare clic sul pulsante *Crea visualizzazione Active Views*.

3. Nella finestra di visualizzazione eventi di Wizard, fare clic sulle frecce giù per selezionare l'asse Z, il Filtro e Visualizzare gli eventi? (Sì o No).

NOTA: Nella finestra di selezione del filtro è possibile creare un filtro personalizzato oppure selezionarne uno esistente. Se si seleziona il filtro "Tutti", nella finestra saranno visualizzati tutti gli eventi. Quando si crea una visualizzazione Active Views, se il filtro assegnato viene modificato o eliminato al termine della creazione, la visualizzazione Active Views rimane invariata.

Dopo aver effettuato la selezione, fare clic su Avanti o su Fine. Se si seleziona Fine, verranno impostati i valori di default seguenti:

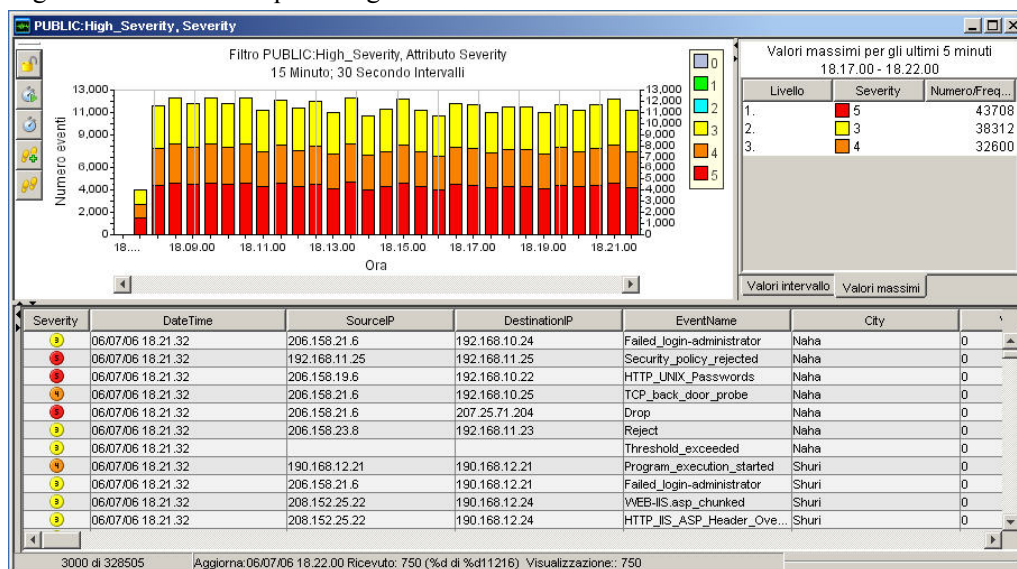
- Visualizzazione e Frequenza di aggiornamento di 30 secondi
- Tempo di visualizzazione di 15 minuti
- Asse Y come Numero eventi
- Tipo di grafico: a barre in pila 2D

4. Se si fa clic su Avanti, fare clic sulle frecce giù per selezionare i parametri seguenti:
   - Visualizzazione e Frequenza di aggiornamento: numero di secondi per la frequenza di aggiornamento da aggiornare
   - Tempo di visualizzazione: intervallo di tempo in cui visualizzare il grafico
   - Asse Y: Numero eventi o Numero eventi al secondo.

   Fare clic su *Avanti*.
5. Selezionare il tipo di grafico. Fare clic *su Avanti*.
   - Tipo di grafico: a barre 3D, in pila 2D, a linee o a nastri
6. Oltre a poter scegliere il filtro, è inoltre possibile perfezionare la tabella eventi. Sono disponibili le condizioni delle opzioni seguenti:
   - Nessuno
   - corrisponde a
   - non è
   - è < (è minore di)
   - è <= (è minore o uguale a)
   - è > (è maggiore di)
   - è >= (è maggiore o uguale a)
   - contiene
   - non contiene
   - è vuoto
   - non è vuoto

   Dopo aver creato i criteri personalizzati, fare clic sul pulsante “*Aggiungi all'elenco*”. Fare clic *su Fine*.

NOTA: Dopo aver creato la visualizzazione personalizzata, è possibile modificare o rimuovere i parametri personalizzati alla tabella degli eventi facendo clic con il pulsante destro del mouse nell'area del grafico e selezionando le proprietà. Per ulteriori informazioni, vedere Riprisitino parametri, Tipo di grafico oppure Tabella eventi di una visualizzazione Active Views.

Il grafico sarà simile a quello seguente:

NOTA: Proprietà visualizzazione Active Views: Rifinisci tabella eventi non si ripercuote sulla rappresentazione grafica.

I cinque pulsanti a sinistra del grafico consentono di eseguire le funzioni seguenti:

- Blocca/Sblocca grafico: utilizzato per l'esecuzione di azioni di drill-down, ingrandimento, riduzione, zoom su selezione e salvataggio di un grafico come file HTML.

- Aumenta intervallo di visualizzazione: aumenta l'intervallo di visualizzazione per gli eventi in ingresso

- Riduci intervallo di visualizzazione: riduce l'intervallo di visualizzazione per gli eventi in ingresso

- Aumenta tempo di visualizzazione: aumenta l'intervallo di tempo lungo l'asse X

- Riduci tempo di visualizzazione: riduce l'intervallo di tempo lungo l'asse X

Quando si fa clic sul *pulsante* Blocca, sono disponibili ulteriori pulsanti:

- Blocca/Sblocca grafico: utilizzato per l'esecuzione di azioni di drill-down, ingrandimento, riduzione, zoom su selezione e salvataggio di un grafico come file HTML.

- Ingrandisci: effettua l'ingrandimento senza modificare le impostazioni relative agli intervalli di tempo del grafico

- Riduci: effettua la riduzione senza modificare le impostazioni relative agli intervalli di tempo del grafico

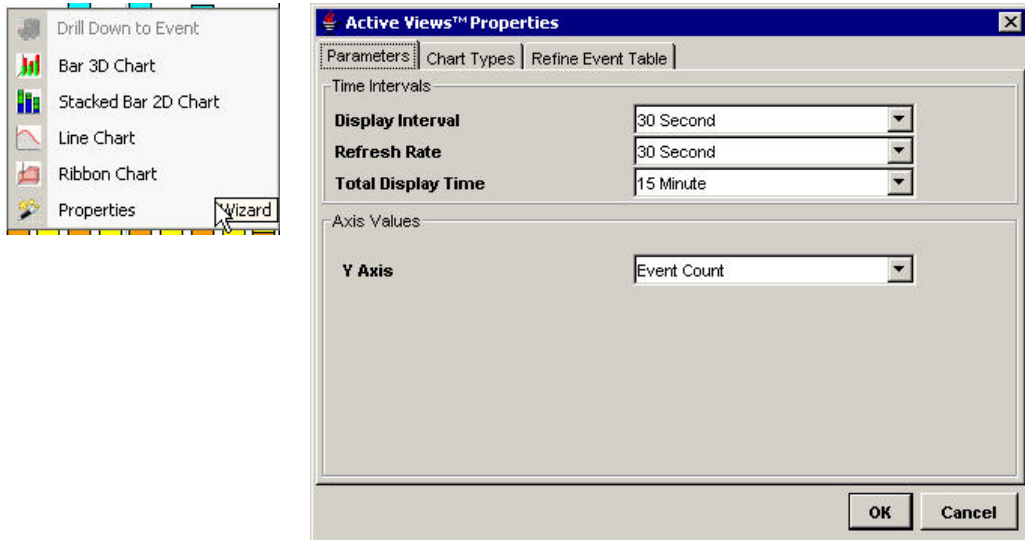
- Zoom su selezione: ingrandisce una selezione di intervalli di tempo degli eventi.

- Salva i dettagli della navigazione come file HTML con il grafico come immagini e gli eventi sotto forma di tabella.

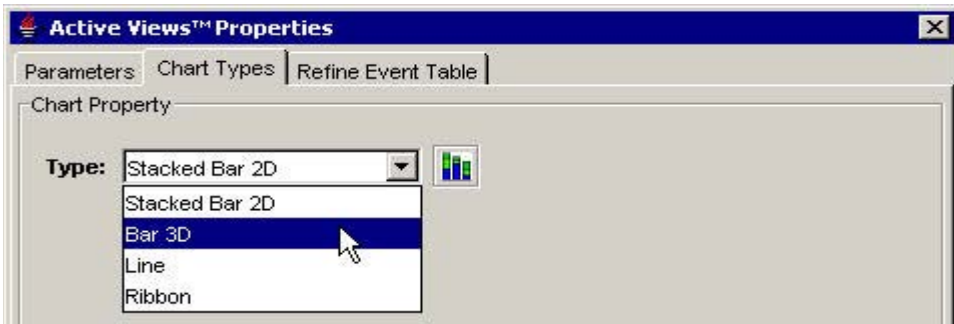
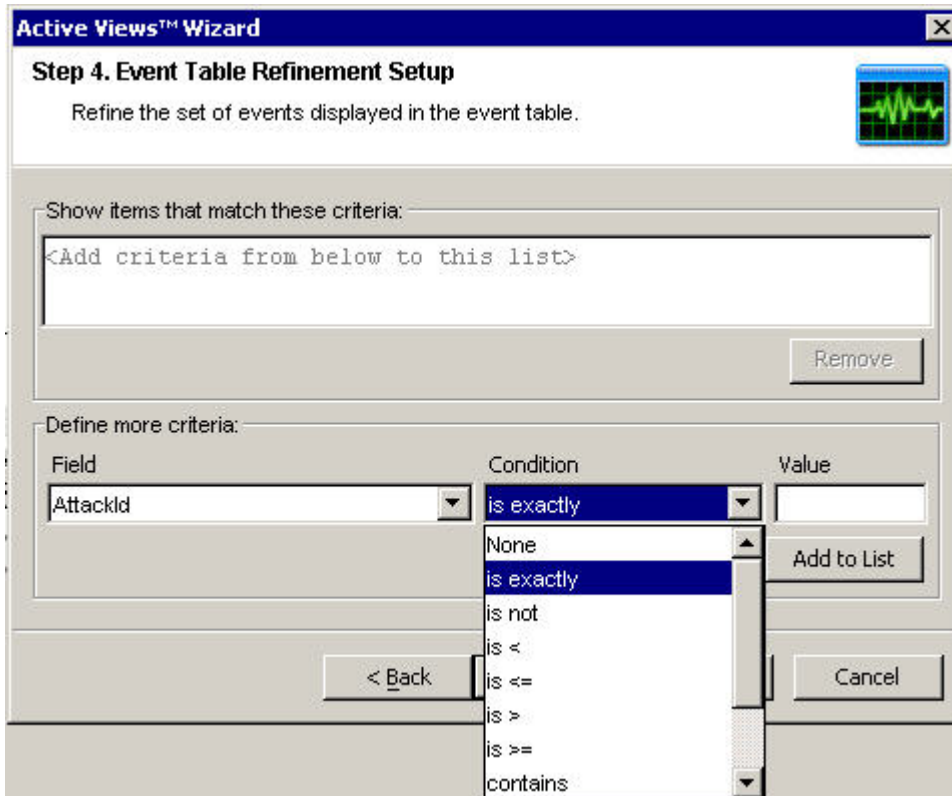
Per ripristinare i Parametri, il Tipo di grafico o la Tabella eventi di una visualizzazione Active Views

Quando si visualizza Active Views, è possibile ripristinare i parametri del grafico, modificare il tipo di grafico e, in caso di eventi di interesse, è possibile filtrare gli altri eventi in modo da creare una nuova visualizzazione Active Views e un filtro.

Per ripristinare i Parametri, il Tipo di grafico o la Tabella eventi di una visualizzazione Active Views

1. All'interno di una visualizzazione Active Views in cui è visualizzato un grafico, fare clic con il pulsante destro del mouse e selezionare *Proprietà*.

Nella scheda Parametri è possibile impostare i valori seguenti:

- Intervallo di visualizzazione: tempo intercorso tra ciascun intervallo
- Frequenza di aggiornamento: numero di secondi per la frequenza di aggiornamento da aggiornare
- Tempo di visualizzazione totale: intervallo di tempo in cui visualizzare il grafico
- Asse Y: Numero eventi o Numero eventi al secondo.

Nella scheda Tipi di grafico è possibile impostare la scelta del grafico a barre 3D, in pila 2D, a linee o a nastri.

In Rifinisci tabella eventi è possibile filtrare il campo Evento all'interno della visualizzazione Active Views.

Ad esempio, è possibile filtrare gli eventi con una voce specifica nel campo, ad esempio DeviceAttackName corrisponde a Back_Door_Probe (TCP 3128). In questo modo nella tabella Eventi saranno contenuti solo gli eventi con DeviceAttackName equivalente a Back_Door_Probe (TCP 3128).

206.158.21.6	192.168.10.25	TCP_back_door_probe
206.158.21.6	192.168.10.25	TCP_back_door_probe

f 564) (DeviceAttackName is exactly Back_Door_Probe (TCP 3128))

Quando si rifinisce una tabella eventi, in basso a destra saranno visualizzati i criteri del filtro.

Rotazione di un grafico a barre 3D o a nastri

Per ruotare un grafico a barre 3D o a nastri

1. Fare clic in un punto qualsiasi del grafico e tenere premuto il pulsante del mouse.
2. Riposizionare il grafico come desiderato spostando il mouse e tenendo premuto il pulsante.

Visualizzazione dei dettagli sugli eventi

Per visualizzare i dettagli degli eventi

1. In una tabella Tempo reale eventi della barra di spostamento visiva o dell'Istantanea, fare doppio clic o clic *con il pulsante* destro del mouse su un evento e fare clic su

Mostra dettagli. Nel pannello di sinistra della tabella Tempo reale eventi saranno visualizzati i dettagli dell'evento.

2. Se si desidera visualizzare i dettagli nell'istanza successiva di Sentinel Control Center, fare clic su *File > Salva preferenze* oppure fare clic sul pulsante *Salva preferenze utente*.

Per nascondere i dettagli di un evento

1. In una tabella Tempo reale eventi della barra di spostamento visiva o dell'Istantanea, con i dettagli dell'evento visualizzati nel pannello di sinistra, fare clic con il pulsante destro del mouse su un evento e poi su *Mostra dettagli*. La finestra relativa ai dettagli dell'evento verrà chiusa.
2. Se non si desidera visualizzare i dettagli nell'istanza successiva di Sentinel Control Center, fare clic su *File > Salva preferenze* oppure fare clic sul pulsante *Salva preferenze utente*.

Invio di messaggi sugli eventi e i casi via e-mail

La possibilità di inviare messaggi di e-mail viene impostata nel file execution.properties durante l'installazione. È possibile modificare questo file dopo l'installazione. Il file è ubicato:

Per Windows:

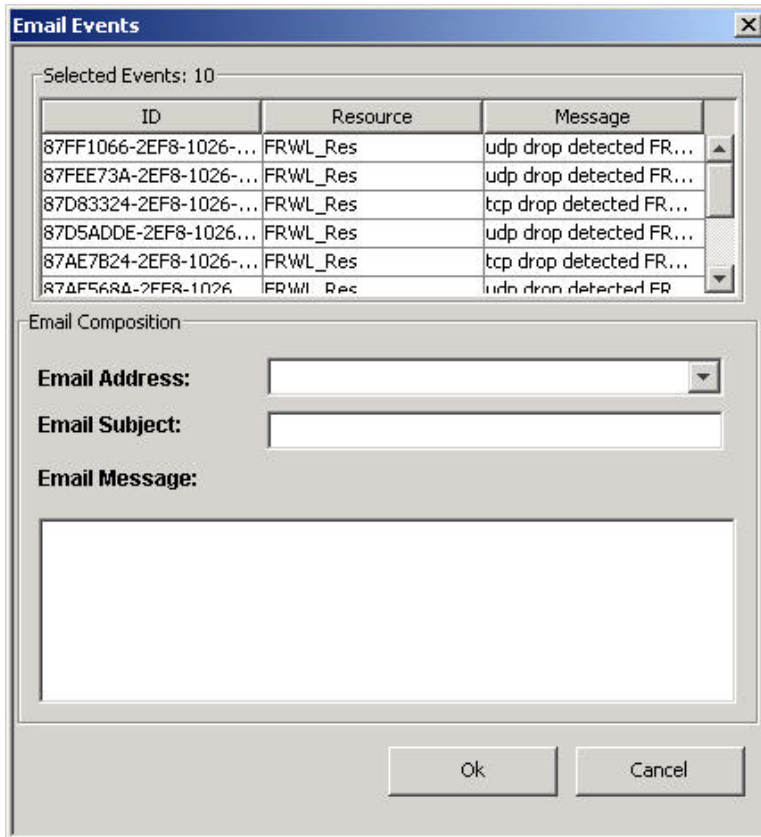
```
%ESEC_HOME%\sentinel\config
```

Per UNIX:

```
$ESEC_HOME/sentinel/config
```

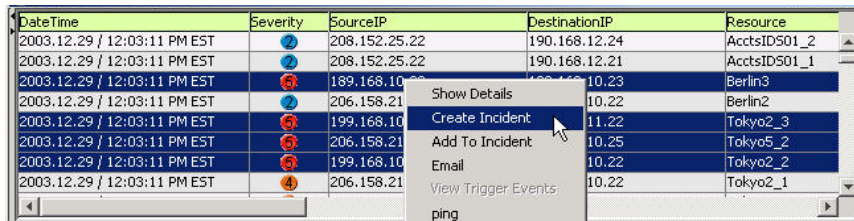
Per ulteriori informazioni, vedere la sezione sulla configurazione di e-mail in Sentinel nel capitolo 11 “Utility”.

Per inviare un messaggio relativo a un evento via e-mail

1. In una tabella Tempo reale eventi della barra di spostamento visiva o dell'Istantanea, selezionare un evento o un gruppo di eventi, fare clic con il pulsante destro del mouse e selezionare *E-mail.*

2. Compilare i campi seguenti:
   - Indirizzo di e-mail
   - Oggetto e-mail
   - Messaggio e-mail
3. Fare clic su *OK*.

Per inviare un messaggio relativo a un caso via e-mail

1. Dopo aver salvato il caso, fare clic sulla *scheda Casi* > *“Visualizza Gestione visualizzazione caso”*.
2. Fare doppio clic su *“Tutti i casi”*.
3. Fare doppio clic su un caso.
4. Fare clic sul pulsante Invia caso *tramite e-mail* .
5. Immettere:
   - Indirizzo di e-mail
   - Oggetto e-mail
   - Messaggio e-mail
6. Fare clic su *OK*. Nel messaggio di e-mail verranno inseriti allegati in formato HTML contenenti dettagli sul caso, gli eventi, le risorse, le vulnerabilità, le informazioni di Advisor e la cronologia.

Creazione di un caso

Per eseguire questa funzione, è necessario disporre dell'autorizzazione dell'utente Crea caso.

Si tratta di una funzione molto utile per raggruppare una serie di eventi per rappresentare un interesse comune (gruppo di eventi analoghi o serie di differenti eventi che indicano uno schema di interesse, ad esempio un attacco).

NOTA: Se all'inizio gli eventi non vengono visualizzati in un caso appena creato, è probabile che si sia verificato un ritardo tra la visualizzazione nella finestra Tempo reale evento e l'inserimento nel database. In questo caso potrebbero essere necessari alcuni minuti affinché gli eventi originali vengano inseriti nel database e vengano visualizzati nel caso.

Per creare un caso

1. In una tabella Tempo reale eventi della barra di spostamento visiva o in una tabella Tempo reale eventi dell'Istantanea, selezionare un evento o un gruppo di eventi, fare clic con il pulsante destro del mouse e selezionare *Crea caso*.

   Nella finestra Nuovo caso sono disponibili le schede seguenti:

   - Eventi: mostra gli eventi che costituiscono il caso
   - Risorse: mostra le risorse interessate
   - Vulnerabilità: mostra le vulnerabilità correlate alle risorse
   - Advisor: attacco alle risorse e informazioni sugli avvisi
   - Workflow: in questa scheda è possibile assegnare un WorkFlow (iTrac)
   - Cronologia: cronologia dei casi
   - Allegati: è possibile allegare documenti o file di testo con informazioni rilevanti al caso

   Nella finestra di dialogo Crea caso, immettere:

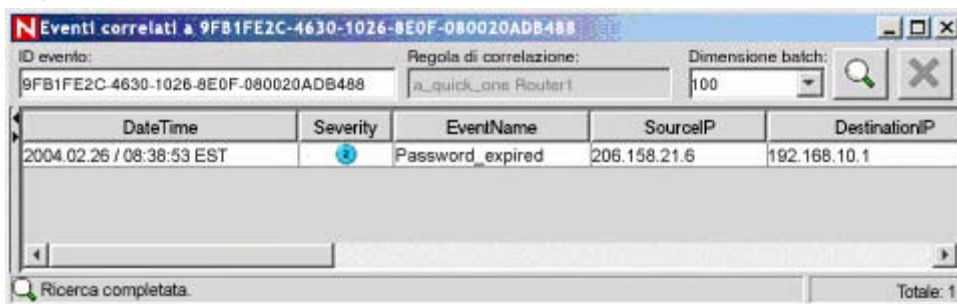
   - Titolo
   - Stato
   - Gravità
   - Priorità
   - Categoria
   - Responsabile: conto utente assegnato al caso
   - Descrizione
   - Risoluzione

2. Fare clic su *Salva*. Il caso viene aggiunto nella scheda Casi di Sentinel Control Center.

Visualizzazione eventi che attivano un Evento correlato

È necessario fare clic con il pulsante destro del mouse su un evento correlato per visualizzare gli eventi che attivano l'evento correlato. Nella tabella degli eventi dalla quale si sta selezionando l'evento, cercare nel pannello di visualizzazione riepilogativo di destra un evento con la proprietà SensorType impostata con un Valore pari a C (C: evento correlato) oppure W (W: watchlist).

Per visualizzare gli eventi che attivano un evento correlato

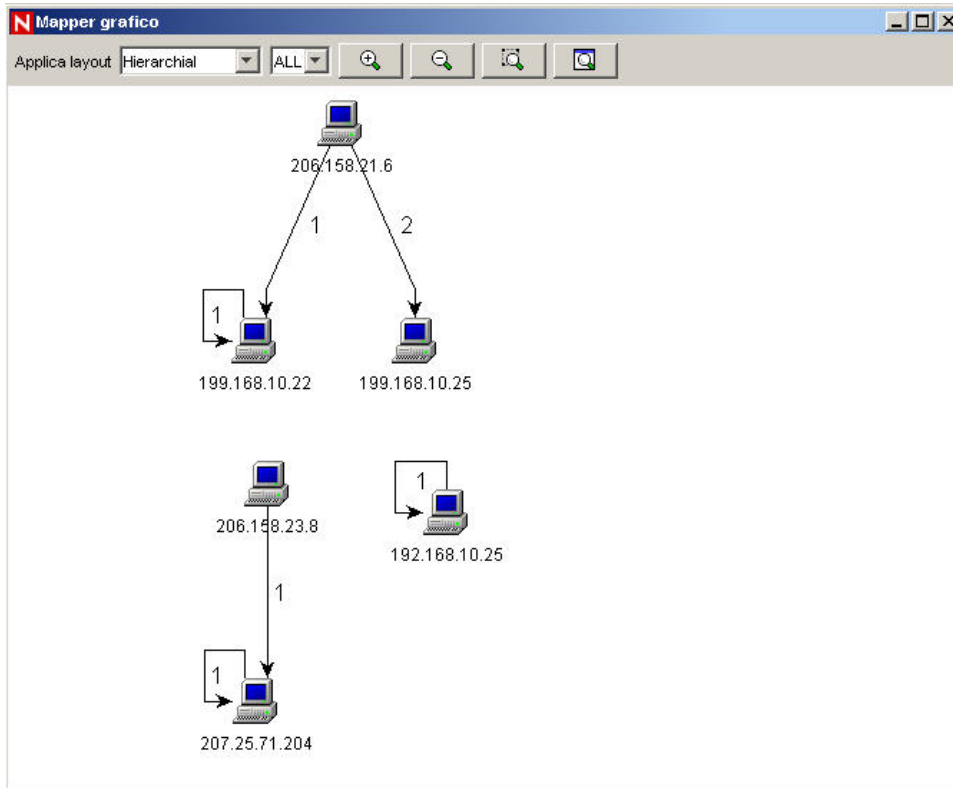
1. In una tabella Tempo reale eventi della barra di spostamento visiva o dell'Istantanea, o in una tabella Interrogazione eventi, fare clic con il pulsante destro del mouse su un evento correlato e selezionare Visualizza eventi trigger. Verrà visualizzata una finestra in cui sono visualizzati gli eventi che hanno attivato la regola e il nome della Regola di correlazione.

Analisi di un evento o di eventi

Questa funzione consente di:

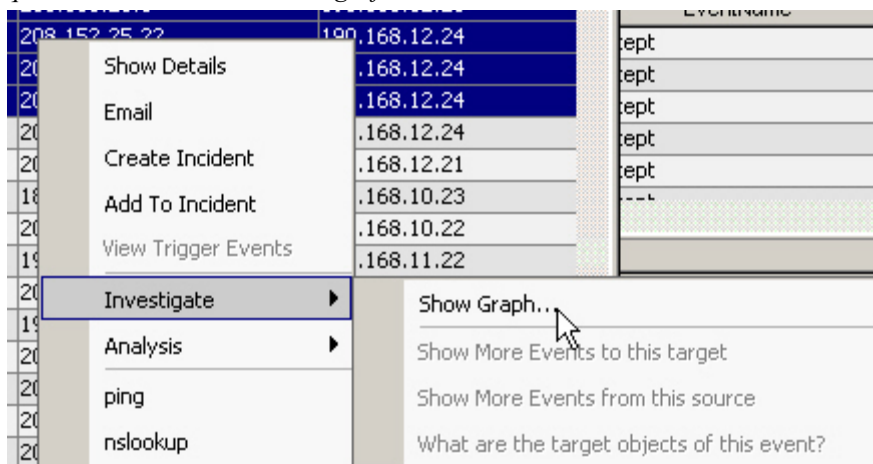
- Visualizzare a livello grafico i campi di origine (IP, porta, evento, tipo sensore, nome Servizio di raccolta e così via) mappati sui campi di destinazione (IP, porta, evento, tipo sensore, nome Servizio di raccolta e così via) degli eventi selezionati.
- Eseguire una Interrogazione eventi per l'ultima ora su un singolo evento per:

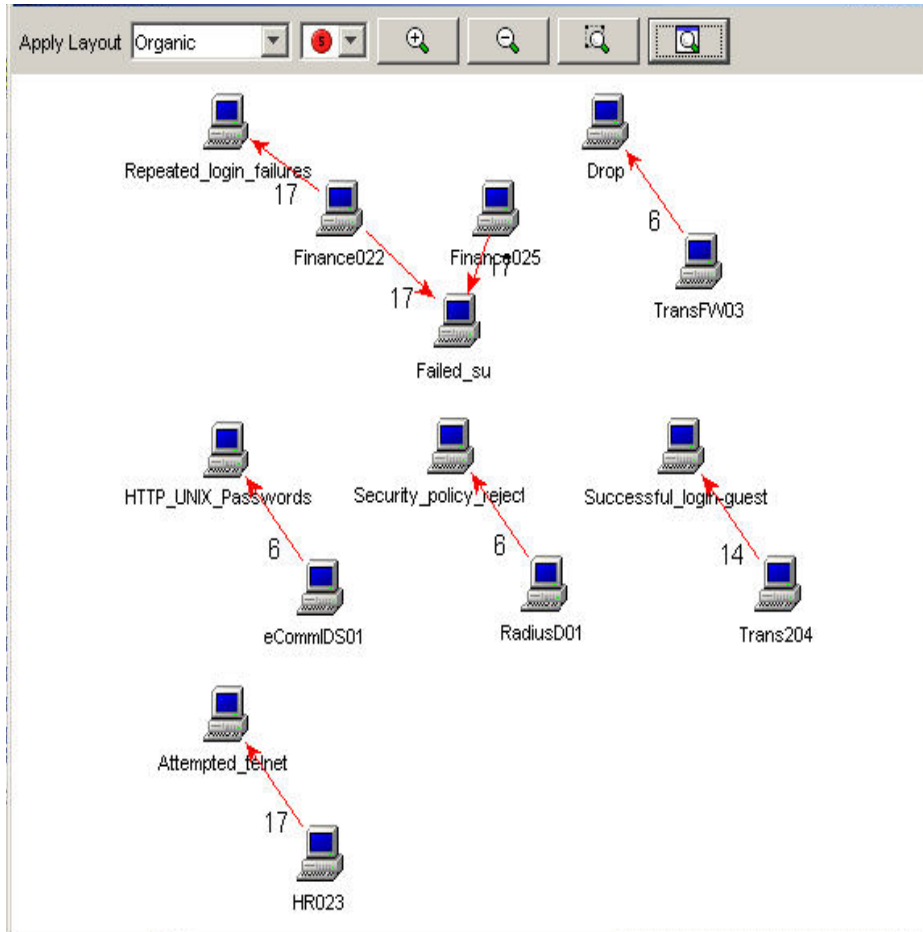
NOTA: Non è possibile eseguire un'interrogazione su un campo nullo (vuoto).

  - Indirizzi IP di destinazione
  - Indirizzi IP di origine
  - Nome evento

Un'illustrazione degli indirizzi IP di origine negli indirizzi IP di destinazione è riportata di seguito.

Analizza: mapper grafico

Per creare una mappa grafica

1. In una tabella Tempo reale eventi della barra di spostamento visiva o della finestra dell'Istantanea, fare clic con il pulsante destro del mouse su un evento o su *più eventi, quindi su Analizza > Mostra grafico*.

Di seguito è illustrata una descrizione grafica di nome del sensore in Nome evento di gravità 5 in un formato organico. La mappatura grafica può essere visualizzata nei formati seguenti:

- Circolare
- Gerarchico
- Organico
- Ortogonale

Analizza: Interrogazione eventi

Questa funzione consente di eseguire un'interrogazione degli eventi occorsi nell'ultima ora.

Per eseguire una Interrogazione eventi utilizzando la funzione Analizza .

1. Nella barra di spostamento visiva o nella finestra dell'Istantanea, fare clic con il pulsante destro del mouse su un evento, *quindi su > Analizza e selezionare una delle tre opzioni illustrate di seguito.*

Opzione	Funzione
Mostra altri eventi per questa destinazione	Indirizzo IP di destinazione
Mostra altri eventi di questa origine	Indirizzo IP di origine
Selezionare gli oggetti di destinazione di questo evento	Nome evento

Analisi: Visualizzazione dei dati Advisor

In Advisor è incluso un riferimento incrociato tra le firme degli attacchi IDS in tempo reale e la Knowledge Base dell'applicazione relativa alle vulnerabilità. In Advisor sono disponibili feed di dati per avvisi e attacchi. Nel feed relativo agli avvisi sono contenute informazioni sulle vulnerabilità e i virus. Nel feed relativo agli attacchi sono elencati gli exploit associati alle vulnerabilità.

I sistemi di rilevamento delle intrusioni supportati sono:

- Cisco Secure IDS
- Enterasys Dragon Host Sensor
- Enterasys Dragon Network Sensor
- ISS BlackICE PC Protection
- ISS RealSecure Desktop
- ISS RealSecure Network
- ISS RealSecure Server Sensor
- ISS RealSecure Guard
- Snort/Sourcefire
- Symantec ManHunt
- Symantec Intruder Alert
- McAfee IntruShield

Il Servizio di raccolta IDS inserisce i dati nel campo DeviceAttackName (rt1) di un evento. Advisor utilizza queste informazioni per generare informazioni sugli attacchi e le vulnerabilità. Alcuni esempi di vulnerabilità:

- FINGER: Cfinger Search Probe
- SMTP: SmartServer3 MAIL FROM Buffer Overflow
- HTTP: Dragon Fire IDS Web Interface Remote Execution
- FTP:MKDIR-DOS
- hp-printer-flood
- wh00t-backdoor
- nt-telnet
- FINGER / tentativo di esecuzione
- tellurian-tftpdnt-filename-bo
- FTP MKD Stack Overflow

Per visualizzare i dati Advisor

1. In una tabella Tempo reale eventi della barra di spostamento visiva o dell'Istantanea, fare clic con il pulsante destro del mouse su un evento o una serie di eventi selezionati, quindi scegliere *Analisi e poi Dati Advisor*. Se il campo Device AttackName è correttamente compilato, verrà visualizzato un rapporto simile a quello riportato di seguito. Questo esempio è per un furto cookie con un clic WEB-MISC amazon.

Analisi: Visualizzazione Dati risorsa

Questa funzione consente di visualizzare e salvare la visualizzazione come file HTML del rapporto sulle risorse. Per visualizzare questi dati è necessario eseguire il Servizio di raccolta di gestione delle risorse. È possibile visualizzare i dati seguenti:

Hardware

- Indirizzo MAC
- Nome
- Tipo
- Fornitore
- Prodotto
- Versione
- Valore
- Criticità
- Riservatezza
- Ambiente
- Ubicazione

Rete

- Indirizzo IP
- Nome host

Software

- Nome
- Tipo
- Fornitore
- Prodotto
- Versione

Contatti

- Ordine
- Nome
- Ruolo
- E-mail
- Numero di telefono

Ubicazione

- Stanza
- Rack
- Indirizzo

Per visualizzare i Dati risorsa

1. In una tabella Tempo reale eventi della barra di spostamento visiva o della finestra dell'Istantanea, fare clic con il pulsante destro del mouse su un evento o più eventi, quindi scegliere Analisi e poi Dati risorsa. Verrà visualizzata una finestra simile a quella seguente.

Asset Report

desk.acmeinc.net

Hardware

MAC Address	A0:12:56:78:90:00		
Name	Build Machine	**Value**	500
Type	Server	**Criticality**	High
Vendor	Dell	**Sensitivity**	Low
Product	Precision	**Environment**	Production
Version	360	**Location**	Internal

Network

IP	Hostname
199.16.2.23	desk.acmeinc.net

Software

Name	Type	Vendor	Product	Version
ClearCase	APPLICATION	IBM	ClearCase	5.0
C++	APPLICATION	Microsoft	Visual C++	6.0

Contacts

Order	Name	Role	Email	Phone Number
1	Erickson, Stein	USER	serickson@acmedomain.net	(703) 555-8865
2	IT	Administrator	LAN_FOLKS@acemedomain.net	(703) 555-9876

Location

Room	server room
Rack	#17
Address	HQ Agent 86 Security Circle Suite 86 Washington DC 12345 USA

Analisi: Visualizzazione delle vulnerabilità

Novell ha disponibili Servizi di raccolta che elaborano le scansioni delle vulnerabilità dalle scansioni Nessus, ISS, Foundstone, eEye e Qualys. La visualizzazione delle vulnerabilità offre una rappresentazione grafica dei dati di eventi in tempo reale sui sistemi vulnerabili ed è disponibile su un evento per le vulnerabilità correnti e di durata evento.

Questa funzione recupera e visualizza i dati relativi alle vulnerabilità per l'IP di destinazione degli eventi selezionati. Per ulteriori informazioni, vedere la documentazione del Servizio di raccolta in formato pdf che si trova in %ESEC_HOME%\wizard\elements\<nome Servizio di raccolta>\doc. Per ottenere i dati sulle vulnerabilità, uno dei servizi di raccolta delle scansioni deve essere caricato e in esecuzione.

NOTA: Il Servizio di raccolta delle vulnerabilità è un Servizio di raccolta delle informazioni e non degli eventi.

La visualizzazione vulnerabilità può essere visualizzata in:

- HTML
- grafico
  - circolare (organico)
  - gerarchico
    - tutte
    - nodi mappati sugli eventi
  - ortogonale

La visualizzazione HTML è una visualizzazione di tipo rapporto in cui sono elencati:

- IP
- host
- vulnerabilità
- porta/protocollo

Di seguito è riportato un esempio di una scansione Nessus.

Vulnerability Summary

<table>
<tr><th>IP</th><th>Host</th><th>Vulnerabilities</th><th>Port/Protocol</th></tr>
<tr><td>172.16.0.132</td><td></td><td>18</td><td>0|)/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh|/TCP, 22(ssh)/TCP, 22|ssh)/TCP, 23(telnet|/TCP, 23|telnet)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587|submission)/TCP, 1241(nessus)/TCP, 1241|nessus|/TCP, 3306(mysql)/TCP</td></tr>
<tr><td>172.16.0.71</td><td></td><td>49</td><td>0|)/TCP, 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 23(telnet)/TCP, 23|telnet)/TCP, 23(telnet)/TCP, 25|smtp)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25|smtp)/TCP, 25|smtp)/TCP, 25|smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 90(dnsix)/TCP, 90(dnsix|/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90|dnsix)/TCP, 90(dnsix)/TCP, 90|dnsix)/TCP, 111(sunrpc)/TCP, 111|sunrpc)/TCP, 161|snmp)/UDP, 512(exec|/TCP, 513(login)/TCP, 514|shell|/TCP, 587(submission|/TCP, 587(submission|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587|submission)/TCP, 587|submission)/TCP, 587(submission|/TCP, 587(submission|/TCP, 587(submission)/TCP, 587(submission)/TCP, 6000(x11)/TCP, 7100(font-service)/TCP, 32778(sometimes-rpc19)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP</td></tr>
<tr><td>172.16.0.132</td><td></td><td>18</td><td>0|)/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh|/TCP, 22(ssh)/TCP, 22|ssh)/TCP, 23(telnet|/TCP, 23|telnet)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587|submission)/TCP, 1241(nessus)/TCP, 1241|nessus|/TCP, 3306(mysql)/TCP</td></tr>
<tr><td>172.16.0.71</td><td></td><td>49</td><td>0|)/TCP, 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 23(telnet)/TCP, 23|telnet)/TCP, 23(telnet)/TCP, 25|smtp)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 25|smtp)/TCP, 25|smtp)/TCP, 25|smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp|/TCP, 25(smtp|/TCP, 90(dnsix)/TCP, 90(dnsix|/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90|dnsix)/TCP, 90(dnsix)/TCP, 90|dnsix)/TCP, 111(sunrpc)/TCP, 111|sunrpc)/TCP, 161|snmp)/UDP, 512(exec|/TCP, 513(login)/TCP, 514|shell|/TCP, 587(submission|/TCP, 587(submission|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587|submission)/TCP, 587|submission)/TCP, 587(submission|/TCP, 587(submission|/TCP, 587(submission)/TCP, 587(submission)/TCP, 6000(x11)/TCP, 7100(font-service)/TCP, 32778(sometimes-rpc19)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP</td></tr>
</table>

La visualizzazione grafica è un rendering delle vulnerabilità che le collega a un evento tramite porte comuni. Di seguito è riportato un esempio di quattro visualizzazioni disponibili.

dnsix
90/TCP
ftp
21/TCP
190.168.12.24
telnet
23/TCP
199.168.10.22
199.168.10.25
dnsix
90/TCP
189.168.10.22
HQ-Scanner-01
199.168.11.22
dnsix
90/TCP
189.168.10.23
190.168.12.21
sometimes-rpc21
32779/TCP
ftp
21/TCP

Organico

HQ-Scanner-01
9.168.10.22
189.168.10.23
190.168.12.21
190.168.12.24
199.168.10.22
199.168.10.25
199.168.11
dnsix
90/TCP
sometimes-rpc21
32779/TCP
ftp
21/TCP
dnsix
90/TCP
ftp
21/TCP
telnet
23/TCP
dnsix
90/TCP

Gerarchico

Circolare

Ortogonale

Nella visualizzazione grafica ci sono quattro pannelli, ovvero:

- pannello grafico
- pannello ad albero
- pannello di controllo
- pannello dettagli/eventi

La visualizzazione del pannello grafico associa le vulnerabilità a una combinazione di porta/protocollo di una risorsa (indirizzo IP). Ad esempio, se una risorsa ha cinque combinazioni univoche di porta/protocollo che sono vulnerabili, alla risorsa saranno collegati cinque nodi. Le risorse sono raggruppate sotto la scansione che ha eseguito l'analisi delle risorse e ha segnalato le vulnerabilità. Se vengono utilizzate due scansioni differenti (ISS e Nessus), ci saranno due nodi di scansione indipendenti a cui saranno associate le vulnerabilità.

NOTA: La mappatura degli eventi viene eseguita solo tra gli eventi selezionati e i dati di vulnerabilità restituiti.

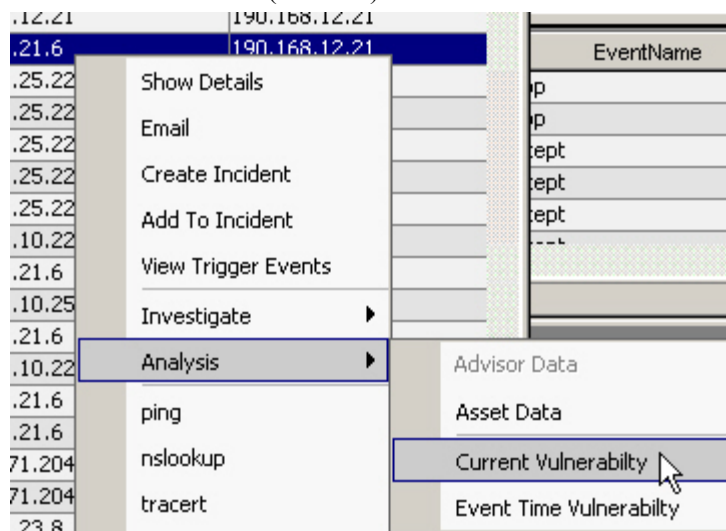
Il pannello ad albero organizza i dati nella stessa gerarchia del grafico. Il pannello ad albero consente inoltre agli utenti di nascondere/mostrare i nodi a qualsiasi livello della gerarchia.

Il pannello di controllo espone tutte le funzionalità disponibili nella visualizzazione, tra cui i seguenti:

- quattro algoritmi differenti di visualizzazione
- capacità di visualizzare tutti i nodi o i nodi selezionati a cui sono mappati degli eventi
- ingrandire o ridurre le aree selezionate del grafico

Nel pannello Dettagli/Eventi, sono disponibili due schede. Nella scheda Dettagli, se si fa clic su un nodo verranno visualizzati i dettagli del nodo. Nella scheda Eventi, se si fa clic su un evento associato a un nodo, il nodo sarà visualizzato sotto forma di tabella, come nella finestra Tempo reale o Interrogazione eventi.

Per eseguire una visualizzazione delle vulnerabilità

1. In una tabella Tempo reale eventi della barra di spostamento visiva o dell'Istantanea, fare clic con il pulsante destro del mouse su un evento o una serie di eventi selezionati, quindi fare clic su:
   - Analisi
     - Vulnerabilità corrente: esegue un'interrogazione del database per le vulnerabilità che sono attive (effettive) alla data e ora correnti.
     - Vulnerabilità ora evento: esegue un'interrogazione del database per le vulnerabilità che erano attive (effettive) alla data e ora dell'evento selezionato.

2. Nella parte inferiore della finestra dei risultati delle vulnerabilità, fare clic su:
   - Evento per grafico vulnerabilità, oppure
   - Rapporto vulnerabilità
3. (Per Evento per grafico vulnerabilità) All'interno della visualizzazione è possibile eseguire le seguenti azioni:
   - spostare i nodi e le relative etichette
   - utilizzare uno dei quattro algoritmi di layout differenti per visualizzare il grafico
   - mostrare tutti i nodi o solo quelli a cui sono mappati degli eventi
   - applicare il filtro ad albero nella linea dell'evento dove un numero elevato di risorse sono restituite come vulnerabili
   - ingrandire o ridurre le aree selezionate

Integrazione di terze parti

L'integrazione di terze parti consente di inviare eventi da qualsiasi schermata di visualizzazione, compresi casi e oggetti associati, a:

- HP Service Desk
- Remedy

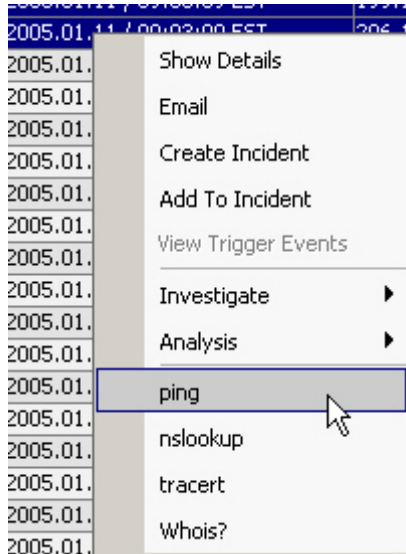
Per inviare un evento singolo o più eventi per software di terze parti

1. In una tabella Tempo reale eventi della barra di spostamento visiva o della finestra dell'Istantanea, a seconda del software di integrazione di terze parti installato, fare clic con il pulsante destro del mouse su un evento e poi su Invia evento a:
   - HP Service Desk
   - Remedy

Utilizzo delle opzioni personalizzate del menu con gli eventi

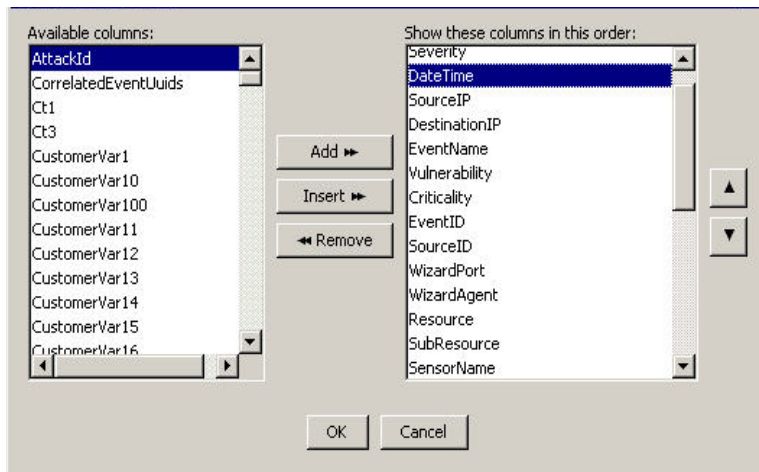
Per utilizzare un'opzione personalizzata del menu con un evento

1. In una tabella Tempo reale eventi esistente della barra di spostamento visiva o dell'Istantanea, selezionare un evento o un gruppo di eventi e fare clic con il pulsante destro del mouse su un'opzione. Verrà visualizzata una finestra di dialogo con le informazioni relative alle opzioni di menu configurate o che consente di inserire le informazioni necessarie per eseguire un'azione. Le opzioni personalizzate di menu di default sono le seguenti:
   - ping
   - nslookup
   - traceroute
   - Whois?

   È possibile assegnare ulteriori autorizzazioni utente per la visualizzazione delle vulnerabilità e le azioni HP. È possibile aggiungere opzioni mediante la finestra Configurazione menu disponibile nella scheda Amministratore.

Gestione delle colonne in un'Istantanea o in una finestra della barra di spostamento visiva

Per selezionare e organizzare le colonne in un'Istantanea o barra di spostamento visiva

1. In una finestra barra di spostamento visiva o Istantanea, fare clic su *Active Views*, *poi su Tempo reale evento e su Gestisci colonne*, oppure su *gestisci colonne* di tabella tempo reale eventi.

2. Utilizzare *i pulsanti Aggiungi e Rimuovi* per spostare i titoli delle colonne tra l'elenco delle Colonne disponibili e le colonne Mostra nell'elenco ordinato. L'opzione Inserisci può essere utilizzata per inserire un elemento di una colonna disponibile in un punto specifico. Ad esempio, nell'illustrazione seguente, se si fa clic sul pulsante *Inserisci*, AttackId sarà posizionato sopra DateTime.

Utilizzare le frecce su e giù per organizzare l'ordine delle colonne come si desidera visualizzarle nella tabella Tempo reale eventi. L'ordine dall'alto in basso dei titoli delle colonne nella finestra di dialogo Gestisci colonne determina l'ordine da sinistra a destra delle colonne nella tabella Tempo reale eventi.

3. Nella finestra di dialogo Gestisci colonne, fare clic su *OK*.
4. Se si desidera visualizzare le colonne nell'istanza successiva di Sentinel Control Center, fare clic su *File > Salva preferenze* oppure fare clic sul pulsante *Salva preferenze utente*.

Creazione di un'istantanea di una finestra barra di spostamento visiva

Per eseguire questa funzione, è necessario disporre dell'autorizzazione dell'utente Istantanea.

È una funzione molto utile per studiare gli eventi di interesse poiché la barra di spostamento visiva viene aggiornata automaticamente ed è possibile scorrere l'avviso o gli avvisi di interesse sullo schermo. All'interno di un'istantanea è inoltre possibile eseguire l'ordinamento per colonne.

Per creare un'istantanea di una tabella Tempo reale eventi

1. In una finestra barra di spostamento visiva o Istantanea, fare clic su *Active Views*, *poi su Tempo reale evento* e su *Istantanea* oppure fare clic *sul pulsante Tabella in tempo reale degli eventi di istantanea* della barra del menu.

Verrà visualizzata una finestra Istantanea che sarà aggiunta all'elenco della cartella Istantanee nella visualizzazione degli eventi della barra di spostamento. La visualizzazione grafica non farà parte dell'Istantanea.

Ordinamento di colonne in un'Istantanea

Per ordinare le colonne in un'Istantanea

1. Fare clic sull'intestazione di una colonna per organizzare l'ordinamento in ordine crescente e doppio clic per organizzarlo in ordine decrescente.

Chiusura di un'Istantanea o di una barra di spostamento visiva

Per chiudere un'Istantanea o una tabella Tempo reale eventi

1. Nella finestra Istantanea o barra di spostamento visiva e se si desidera visualizzare la tabella nell'istanza successiva di Sentinel Control Center, fare clic su *File > Salva preferenze*.
2. Chiudere la tabella mediante il pulsante Chiudi (in alto a destra in Windows o in alto a sinistra in UNIX).

Eliminazione di un'Istantanea o di una barra di spostamento visiva

Per eliminare un'Istantanea o una barra di spostamento visiva

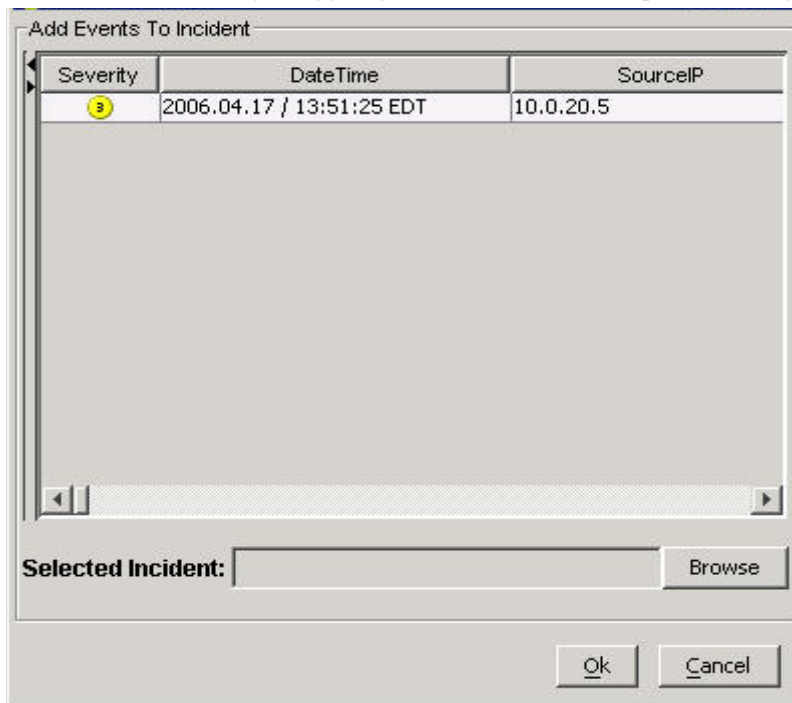
1. Mentre è visualizzata un'Istantanea o una Barra di spostamento visiva, chiudere utilizzando il pulsante Chiudi (in alto a destra in Windows o in alto a sinistra in UNIX).
2. Fare clic su *File, quindi scegliere Salva preferenze* oppure fare clic sul pulsante *Salva preferenze utente*.

La visualizzazione o istantanea non saranno visualizzate quando si chiude e si riapre Sentinel Control Center.

Aggiunta di eventi a un Caso

Per eseguire questa funzione, è necessario disporre dell'autorizzazione dell'utente Crea caso.

Per aggiungere eventi a un caso

1. In una tabella Tempo reale eventi o in un'Istantanea, selezionare un evento o un gruppo di eventi e fare clic con il pulsante destro del mouse per visualizzare e fare clic su “*Aggiungi a caso*”.
2. Nella finestra di dialogo “*Aggiungi a caso*”, fare clic sul pulsante Sfoglia.

3. Fare clic sul pulsante *Sfoglia* per visualizzare un elenco dei casi disponibili.

NOTA: È possibile definire i criteri per eseguire una ricerca dettagliata di uno specifico caso o casi.

4. Fare clic sul pulsante *Cerca per visualizzare un elenco dei casi*.

5. Evidenziare un caso e fare clic sul pulsante *Aggiungi*.
6. Fare clic su *OK*. L'evento o gli eventi selezionati sono aggiunti al caso nella barra di spostamento dei casi.

NOTA: Se all'inizio gli eventi non vengono visualizzati in un caso appena creato, è probabile che si sia verificato un ritardo tra la visualizzazione nella finestra Tempo reale evento e l'inserimento nel database. In questo caso potrebbero essere necessari alcuni minuti affinché gli eventi originali vengano inseriti nel database e vengano visualizzati nel caso.

Scheda Casi

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Per utilizzare la scheda Casi, è necessario disporre dell'autorizzazione appropriata. Se questa autorizzazione non viene assegnata, non saranno disponibili neanche le altre autorizzazioni relative alle azioni eseguibili con questa scheda.

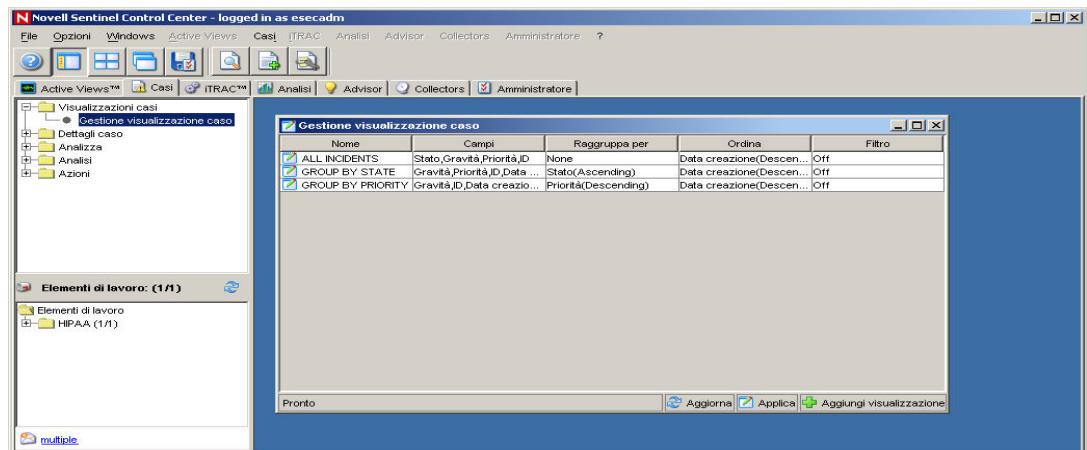
In questo capitolo viene illustrato come gestire i casi. I casi sono raggruppamenti di uno o più eventi di rilievo.

Creazione di casi

- Nella finestra Tempo reale, i casi possono essere selezionati individualmente per creare un nuovo caso oppure aggiunti a un caso esistente.
- I casi possono inoltre essere creati automaticamente, attivando regole di correlazione.

Scheda Casi: Descrizione

Le seguenti operazioni possono essere eseguite per i casi.

- Invio del caso tramite e-mail
- Modifica di un caso
- Visualizzazione di un caso
- Eliminazione di un caso
- Aggiunta di una Visualizzazione caso

Relazione tra eventi e casi

Per evento si intende un'azione o un'occorrenza rilevata da un dispositivo o programma di protezione. Gli eventi sono privi di stato.

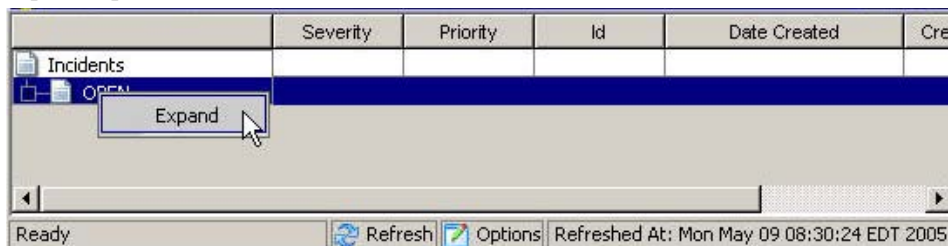
Gli eventi considerati di importanza significativa (un possibile attacco) possono essere raggruppati insieme in un caso. Ai casi sono associati stati che indicano se è necessaria una risposta o la chiusura.

Visualizzazione di un caso

Per visualizzare uno o più casi, è necessario disporre della relativa autorizzazione.

Per visualizzare un caso

1. Fare clic sulla scheda *Casi*.
2. Fare clic su *Casi* > *Visualizza Gestione visualizzazione caso* oppure sul pulsante *Gestione visualizzazione caso* .
3. Nella finestra Gestione visualizzazione caso sono disponibili le seguenti visualizzazioni.
   - Tutti i casi
   - Raggruppa per Stato
   - Raggruppa per Priorità

   Fare doppio clic sul nome di una visualizzazione.
4. Fare clic con il pulsante destro del mouse sul nome selezionato, quindi scegliere *Espandi*, per visualizzare i casi.

Per impostare un'opzione di visualizzazione del caso

1. Fare clic sulla scheda *Casi*.
2. Fare clic su *Casi* > *Visualizza Gestione visualizzazione caso* oppure sul pulsante

Visualizza Gestione visualizzazione caso .

3. Nella finestra Gestione visualizzazione caso, fare doppio clic sul nome di una visualizzazione.

4. Fare clic su *Opzioni*.

In questa finestra è inoltre possibile impostare le opzioni seguenti:

- Campi...
- Raggruppa per...
- Ordina...
- Filtro...
- Visualizzazione albero

Fare clic su *Applica e su Salva*.

5. Nella finestra Gestione visualizzazione caso, fare doppio clic sul nome di una visualizzazione.

Nella figura seguente è illustrata la visualizzazione di default della finestra di visualizzazione di tutti i casi.

	State	Severity	Priority	Id	Responsible
sev4	OPEN	High (4)	None (0)	103	esecadm
mixed severity	OPEN	Medium (3)	None (0)	102	esecadm
sev2	OPEN	Low (2)	None (0)	101	esecadm
sev3	OPEN	Medium (3)	Medium (2)	100	

La visualizzazione seguente è ordinata in base alla gravità, con l'opzione Campi (gestione colonne) delle prime quattro colonne impostata su Gravità, Data creazione, Priorità e Classificazione criticità.

	Severity	Date Created	Priority	Criticality Rating	Severity Rating	Modified By	
sev4	High (4)	05/09/2005 ...	None (0)	0.0	0.0	esecadm	OPEI
mixed severity	Medium (3)	05/09/2005 ...	None (0)	0.0	0.0	esecadm	OPEI
sev2	Low (2)	05/09/2005 ...	None (0)	0.0	0.0	esecadm	OPEI
sev3	Medium (3)	05/09/2005 ...	Medium (2)	0.0	0.0	esecadm	OPEI

La visualizzazione seguente è raggruppata per titolo.

	Severity	Date Created	Priority	Criticality Rating	Severity Rating	Modified By	
Incidents							
mixed severity							
mixed severity	Medium (3)	05/09/2005 ...	None (0)	0.0	0.0	esecadm	OPEI
sev2							
sev3							
sev4							

La visualizzazione ad albero seguente è ordinata in base alla Data creazione.

	Severity	Date Created	Priority	Criticality Rating	Severity Rating	Modified
Incidents						
mixed severity						
05/09/2005 08:44:25 EDT	Medium (3)	05/09/2005 ...	None (0)	0.0	0.0	esecadm
sev2						
05/09/2005 08:44:07 EDT	Low (2)	05/09/2005 ...	None (0)	0.0	0.0	esecadm
sev3						

Aggiunta di una Visualizzazione caso

Quando si aggiunge una Visualizzazione caso, sono disponibili le opzioni seguenti:

- Campi...
- Raggruppa per...
- Ordina...
- Filtro...
- Visualizzazione albero

Per aggiungere una Visualizzazione caso

1. Nella Gestione visualizzazione caso, fare clic sul *pulsante Aggiungi visualizzazione*.

2. Immettere un nome nel campo Nome opzione, selezionare le opzioni necessarie, quindi fare clic su *Salva*.

Campi e dettagli dei casi

Campi dei casi

- Titolo: nome del caso.
- Stato
  - Aperto
  - Riconosciuto
  - Assegnato
  - In fase di analisi
  - Falso positivo
  - Verificato
  - Approvato
  - Chiuso
- Gravità
  - Nessuna (0)
  - Irrilevante (1)
  - Basso (2)
  - Medio (3)
  - Alto (4)
  - Grave (5)
- Priorità
  - Basso (1)
  - Medio (2)
  - Alto (3)
  - Urgente (4)
  - Massima (5)
- Categoria (facoltativa): testo che può essere utilizzato per identificare meglio il caso.
- Responsabile: conto utente assegnato al caso
- Descrizione: testo.
- Risoluzione: testo.

Dettagli dei casi

- Eventi: eventi associati al caso.
- Risorse: elenco di tutte le risorse associate al caso.
- Vulnerabilità: visualizzazione di tutte le vulnerabilità associate al caso.
- Advisor: visualizzazione di tutte le informazioni sugli attacchi associate al caso.
- Workflow: visualizzazione del workflow associato al caso. In questa scheda è possibile assegnare i valori seguenti:
  - Nessuno
  - Processo di conformità alla normativa HIPAA
  - Processo di risposta al caso SANS
  - Processo di conformità al protocollo FTP Sarbanes Oxley
  - Risposta automatica
- Cronologia: cronologia dei casi (elenco di tutte le operazioni eseguite sul caso, comprese l'ora e la data dell'operazione e una breve nota informativa).
- Allegati: è possibile allegare qualsiasi informazione rilevante (documenti o file di testo) al caso.
- Dati esterni.

NOTA: Quando si aggiungono eventi a un caso, nelle schede Risorse/Vulnerabilità/Advisor verrà inserito un elenco di tutti i dati relativi a tali categorie che corrispondono ai nomi dell'IP e dell'host di destinazione degli eventi associati.

NOTA: I pulsanti Aggiungi e Rimuovi delle schede Risorse/Vulnerabilità/Advisor consentono di aggiungere e rimuovere manualmente i dati relativi a tali categorie.

Creazione di un caso

Per creare un caso

1. Fare clic sulla *scheda Caso*.
2. Fare clic su *Casi* > *Crea caso* oppure sul pulsante *Crea un nuovo caso*.

Nella finestra di dialogo Crea caso, immettere le informazioni necessarie nei campi vuoti.

3. Fare clic su *Salva*.

Visualizzazione e salvataggio degli allegati

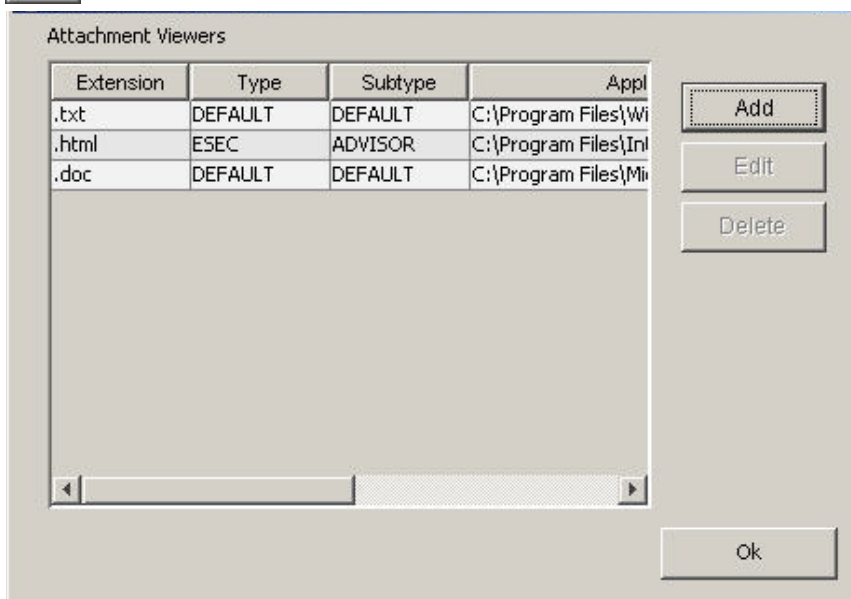
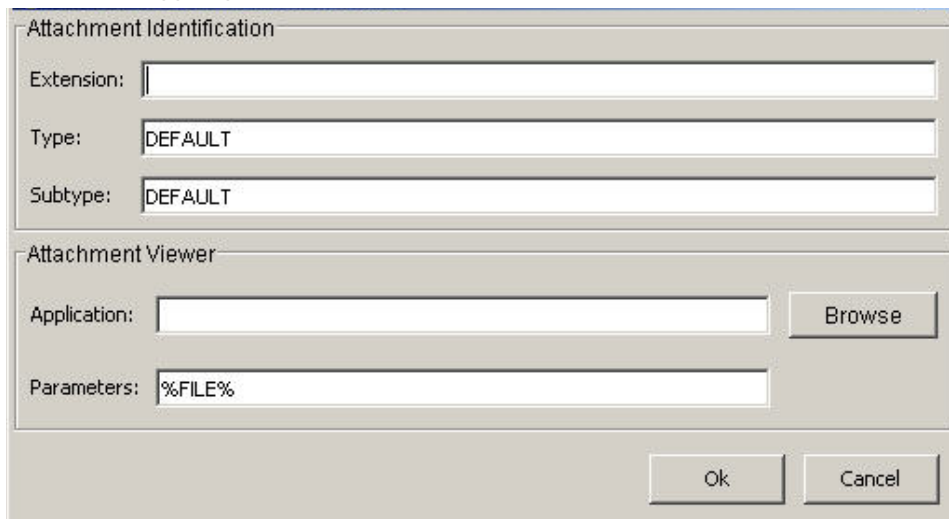
Per visualizzare un allegato

1. Fare clic con il pulsante destro del mouse sull'allegato e scegliere se *visualizzarlo* o *salvarlo*.

NOTA: Per poter visualizzare l'allegato, è necessario che nel computer sia configurato un visualizzatore di allegati. Se così non fosse, verrà visualizzato un prompt che consentirà di scegliere il programma da utilizzare per aprire il file. Gli allegati vengono salvati nel database di Sentinel.

Configurazione del visualizzatore di allegati

Per configurare il visualizzatore di allegati

1. Fare clic sulla *scheda Caso*.
2. Fare clic su *Casi* > *Configurazione visualizzatori di allegati* oppure fare clic sul pulsante *Configura visualizzatori di allegati*.

3. Fare clic su *Aggiungi*.

   Immettere il tipo di estensione, quale .doc, .xls, .txt, .html e così via, quindi fare clic su *Sfoglia* oppure digitare il nome dell'applicazione per avviare il tipo di file (ad esempio, notepad.exe per Blocco note).

4. Fare clic su *OK*.

Invio del caso tramite e-mail

La possibilità di inviare messaggi di e-mail viene impostata nel file execution.properties durante l'installazione. Per configurare questo file, vedere il *Capitolo 11: Utility*.

Per inviare il caso tramite e-mail

1. Fare clic sulla *scheda Casi*.
2. Nella barra di spostamento, se disponibile, espandere la cartella Casi. In alternativa, fare clic su *Casi > Visualizza elenco casi* oppure sul pulsante *omonimo* .
3. Fare doppio clic sul *nome di una Visualizzazione caso*.
4. Fare doppio clic su un caso.
5. Fare clic sul pulsante Invia caso *tramite e-mail* .
6. Immettere:
   - Indirizzo di e-mail
   - Oggetto e-mail
   - Messaggio e-mail
7. Fare clic su *OK*. Nel messaggio di e-mail verranno inseriti allegati in formato HTML contenenti dettagli sul caso, gli eventi, le risorse, le vulnerabilità, le informazioni di Advisor e la cronologia.

Modifica di un caso

Per modificare un caso

1. Fare clic sulla *scheda Casi*.
2. Fare clic su *Casi > Visualizza Gestione visualizzazione caso* oppure sul pulsante *Visualizza Gestione visualizzazione caso* .
3. Fare doppio clic sulla visualizzazione di un caso.
4. Fare doppio clic su un caso.
5. Verrà visualizzata la finestra Dettagli caso.
6. I seguenti campi possono essere modificati (operazione facoltativa):
   - Titolo
   - Stato
   - Gravità
   - Priorità
   - Categoria
   - Responsabile
   - Descrizione
   - Risoluzione
7. Gli allegati possono essere aggiunti o rimossi nella scheda Allegati.
8. Fare clic su *Salva*.

Eliminazione di un caso

NOTA: Per eliminare un caso allegato a un workflow (iTRAC), è necessario interrompere il processo iTRAC.

Per eliminare un caso

1. Fare clic sulla *scheda Casi.*
2. Fare clic su *Casi* > *Visualizza Gestione visualizzazione caso oppure sul pulsante omonimo* .
3. Fare doppio clic sulla visualizzazione di un caso.
4. Nella finestra di visualizzazione dei casi, fare clic con il pulsante destro del mouse su un caso, quindi su Elimina.

   NOTA: Per eliminare un caso allegato a un workflow (iTRAC), è necessario interrompere il processo iTRAC. Tale processo può essere interrotto utilizzando la Gestione visualizzazione processi nella scheda iTRAC. Per ulteriori informazioni, vedere il *Capitolo 5: Scheda iTrac*.

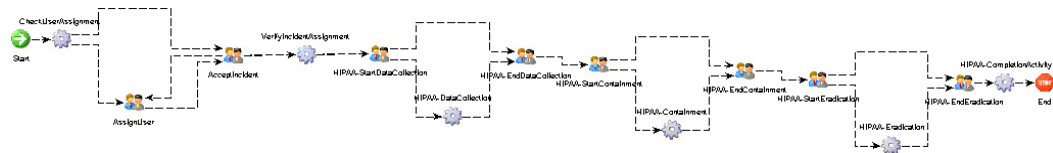
5. Scegliere Sì nella finestra di conferma.

5 Scheda iTRAC™

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

iTRAC (workflow) consente di automatizzare le procedure e rispondere agli eventi indesiderati. Sentinel fornisce un sistema di gestione iTRAC che consente l'automazione procedurale dei processi. iTRAC è collegato al framework dell'attività di Sentinel, che fornisce le attività eseguibili automaticamente in ogni fase del processo iTRAC.

I modelli (definizione dei processi) e l'esecuzione dei processi costituiscono il sistema di gestione del workflow.

Modelli (definizione dei processi)

Il modello è la struttura che controlla il flusso di esecuzione in iTRAC. È composto da una rete di attività e dalle rispettive relazioni, criteri per la transizione tra le attività e le informazioni su ognuna di esse. Gli attributi dei modelli possono essere modificati dall'utente.

iTRAC consente di impostare attributi di timeout in un modello iTRAC.

Un'attività è un'unità di lavoro logica, indipendente all'interno del processo iTRAC. Un'attività rappresenta il lavoro che verrà svolto dagli utenti o dai ruoli (attività manuali) oppure dalle applicazioni del computer (attività automatiche).

Le attività manuali e automatiche inoltre sono caratterizzate da timeout che gli utenti possono abilitare e disabilitare.

Oltre agli attributi di timeout, le attività manuali consentono di configurare l'attributo della risorsa che determina l'utente o il ruolo che esegue tali attività.

Oltre agli attributi di timeout, le attività automatiche consentono di configurare nel framework delle attività Sentinel l'attività automatica da eseguire.

Gestione modelli

iTRAC consente di creare nuovi modelli, manipolare gli attributi dei processi e delle attività nei modelli esistenti ed eliminare i modelli in cui viene utilizzata la finestra Gestione modelli nella scheda iTRAC.

È possibile accedere a Gestione modelli facendo clic sul relativo nodo nella struttura ad albero nella scheda iTRAC.

Modelli di default

iTRAC dispone di quattro modelli di default che includono attività automatiche e manuali. Gli attributi dei processi e delle attività per questi modelli sono stati impostati su valori predefiniti, che gli utenti possono modificare per soddisfare le proprie esigenze. I modelli di default sono:

- HIPAA
- Sarbanes Oxley
- Gestione degli eventi indesiderati SANS
- Risposta automatica

Creazione di nuovi modelli

1. Fare clic sulla scheda *iTRAC*.
2. Nella barra di spostamento fare clic su *Amministrazione iTRAC* > *Gestione modelli*.
3. Evidenziare un processo esistente (HIPAA, Sarbanes-Oxley, SANS o un processo definito dall'utente) e fare clic con il pulsante destro del mouse su *Crea copia*.
4. Immettere un nome.
5. Se si seleziona un timeout, è necessario immettere un indirizzo e-mail e specificare un'ora. L'ora deve essere espressa in numeri interi. È possibile selezionare minuti, secondi, ore o giorni.
6. Inserire una descrizione. Per modificare gli attributi dei processi e delle attività, fare riferimento alla sezione Modifica di modelli esistenti. Fare clic su *OK*.
7. In Personalizzazione modelli, fare clic su *Salva*.

Modifica di modelli esistenti

Durante la modifica di un processo, è possibile modificarne gli attributi o modificare gli attributi delle attività all'interno del processo.

È possibile modificare gli attributi seguenti:

- nome
- periodo di timeout oppure disabilitare il periodo di timeout
- descrizione

Modifica degli attributi di un processo

1. Fare clic sulla scheda *iTRAC*.
2. Nella barra di spostamento fare clic su *Amministrazione iTRAC* > *Gestione modelli*.
3. Evidenziare un modello esistente, fare clic *con il pulsante* destro del mouse e *scegliere Visualizza*.

   Nella finestra del modello fare clic sul pulsante dei dettagli del processo.

4. Nella finestra di dialogo Personalizzazione processi, è possibile modificare le opzioni seguenti:
   - Nome
   - durata (minuti, secondi, ore e giorni)
   - timeout (se abilitato sarà necessario immettere un indirizzo e-mail e specificare un'ora)
   - Descrizione

Modifica di attività manuali

È possibile modificare la risorsa (utente/ruolo), il timeout e la descrizione delle attività manuali.

1. Fare clic sulla scheda *iTRAC*.
2. Nella barra di spostamento fare clic su *Amministrazione iTRAC* > *Gestione modelli*.
3. Evidenziare un modello esistente, fare clic con il pulsante destro del mouse e scegliere Visualizza.
4. Il modello viene visualizzato in una finestra separata.
5. Per apportare le modifiche, fare doppio clic su una delle icone delle attività manuali nel modello.

NOTA: le attività manuali seguenti presenti nei modelli esistenti possono essere modificate come descritto sotto.

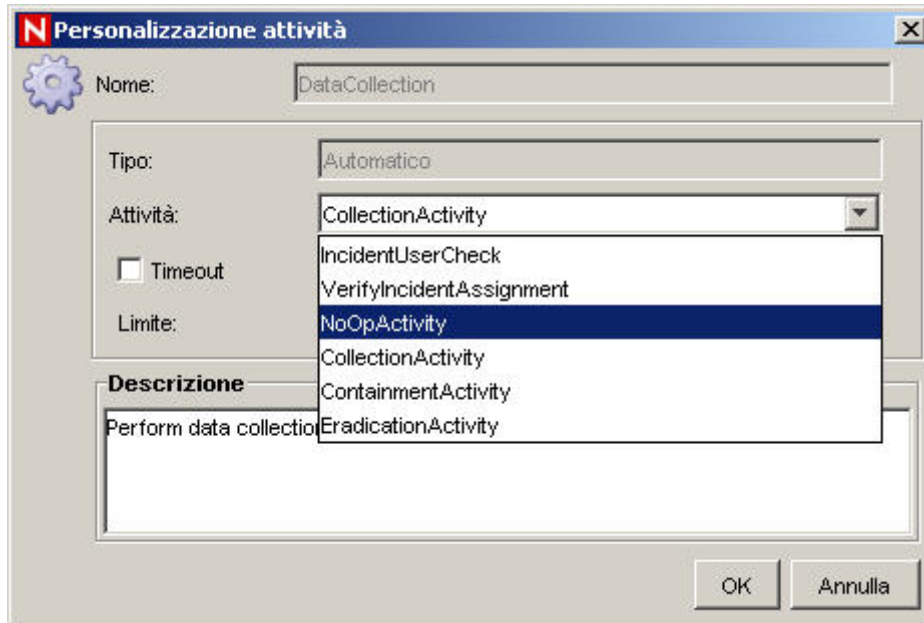
- AssignUser
- AcceptIncident
- ConfirmStartDataCollection
- ConfirmEndDataCollection
- ConfirmStartContainment
- ConfirmEndContainment
- ConfirmStartEradication
- ConfirmEndEradication

Modifica di attività automatiche

È possibile modificare l'attività, il timeout e la descrizione di un'attività automatica.

1. Per apportare le modifiche, fare doppio clic su una delle icone dell'attività automatica nel modello.
2. Nell'elenco a discesa della finestra di dialogo Personalizzazione attività è visualizzato l'elenco delle attività che possono essere utilizzate come attività automatiche. Le attività elencate sono create utilizzando il framework delle attività.

NOTA: le attività automatiche seguenti presenti nei modelli esistenti possono essere modificate come descritto sotto.

- DataCollection
- Containment
- Eradication

Eliminazione di modelli

1. Fare clic sulla scheda *iTRAC*.
2. Nella barra di spostamento fare clic su *Amministrazione iTRAC* > *Gestione modelli*.
3. Evidenziare un modello esistente, quindi fare clic con il pulsante destro del mouse su Elimina.
4. Scegliere *Sì* nel riquadro relativo all'eliminazione del modello.

Esecuzione dei processi

L'esecuzione di un processo è il periodo di tempo durante il quale il processo è operativo e si creano e gestiscono istanze del processo.

Quando si esegue o si crea un'istanza di un processo iTRAC nel server iTRAC, un'istanza del processo viene creata, gestita ed eventualmente terminata nel server iTRAC in conformità con la definizione del processo. Quando il processo sta per essere completato o terminato, vengono eseguite diverse attività definite nel modello del workflow basato sui criteri che regolano le transizioni tra di esse. Nel server del workflow di iTRAC, le attività manuali e automatiche sono elaborate in modo differente.

Un processo iTRAC dipende da un caso Sentinel; un'istanza di processo non può esistere se non c'è un caso a essa collegato. D'altra parte, un caso può esistere senza collegamenti al server del workflow. A un'istanza di un processo iTRAC può essere associato un solo caso.

Creazione di un'istanza di un processo

Nel server iTRAC è possibile creare un'istanza di un processo iTRAC associando a esso un caso in uno dei tre metodi seguenti:

- associazione di un processo iTRAC a un caso in fase di creazione di quest'ultimo
- associazione di un processo iTRAC a un caso in seguito alla creazione di quest'ultimo
- associazione di un processo iTRAC a un caso tramite correlazione

Per ulteriori informazioni sull'associazione di processi a casi, fare riferimento al capitolo in cui è descritta la scheda Casi.

Esecuzione di attività automatiche

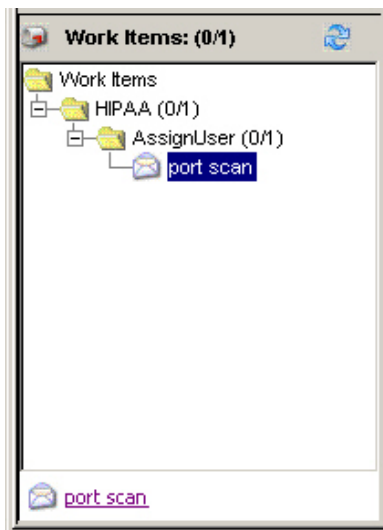
Quando nell'istanza di un processo viene eseguita un'attività automatica, si esegue l'attività associata definita nel modello. L'attività associata è un'attività creata utilizzando il framework delle attività. L'attività viene eseguita nel server iTRAC; il risultato viene memorizzato nelle variabili di processo e nelle transizioni che portano all'attività successiva nel modello iTRAC.

L'attività del framework delle attività, ad esempio, può essere impostata per eseguire il PING su un server e collegare i risultati al caso associato.

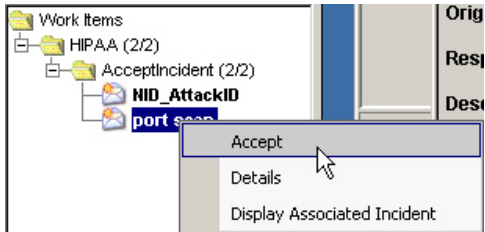
Esecuzione di attività manuali

Se si esegue un'attività manuale, il server iTRAC invia notifiche sotto forma di elementi di lavoro alla risorsa assegnata. Se la risorsa assegnata è un utente, l'elemento di lavoro verrà inviato solo a quell'utente. Se l'attività è stata assegnata a un ruolo, l'elemento di lavoro verrà inviato a tutti gli utenti di quel ruolo. Prima di procedere con l'attività successiva, il server iTRAC attende che l'utente completi l'elemento di lavoro.

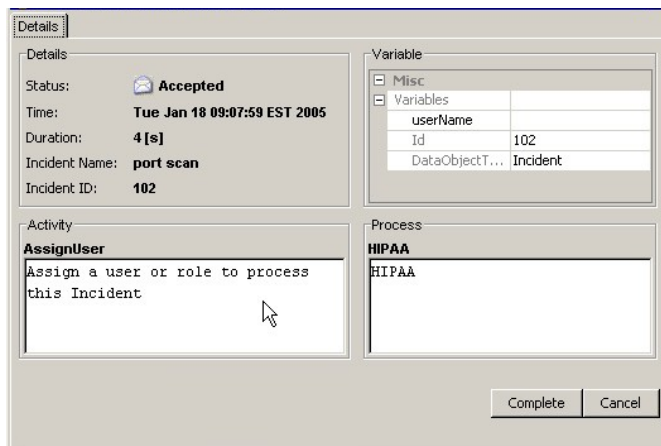
Elenchi di lavoro

Gli elementi di lavoro sono presentati all'utente in un elenco di lavoro, nel quale sono mantenuti i dettagli di tutti gli elementi di lavoro allocati a tale utente. Si tratta dell'elenco delle operazioni che l'utente deve compiere.

L'elenco di lavoro può essere visualizzato in qualsiasi scheda dell'interfaccia utente di Sentinel. Gli elementi di lavoro sono raggruppati in base al processo e all'attività a cui appartengono. Se sono evidenziati in grassetto, significa che non sono ancora stati accettati dall'utente.

Tramite gli elenchi di lavoro, gli utenti possono interagire con i singoli elementi di lavoro.

- Per visualizzare i dettagli degli elementi di lavoro, è possibile fare doppio clic oppure fare clic con il pulsante destro del mouse su Dettagli.
- Con il pulsante destro del mouse è possibile accettare gli elementi di lavoro non accettati.
- Con il pulsante destro del mouse è possibile visualizzare i dettagli del caso associato.

Elementi di lavoro

Un elemento di lavoro costituisce il task che l'utente deve svolgere per l'attività manuale in esecuzione in un processo iTRAC. Il controllo e l'avanzamento dell'elemento di lavoro dipendono dall'utente.

Prima di procedere con l'attività successiva all'interno dell'istanza del processo, il server iTRAC attende che l'utente completi il task.

Nella finestra di dialogo sopra illustrata sono riportate le informazioni seguenti:

- dettagli dell'elemento di lavoro
- variabili dell'elemento di lavoro
- descrizione dell'attività
- descrizione del processo

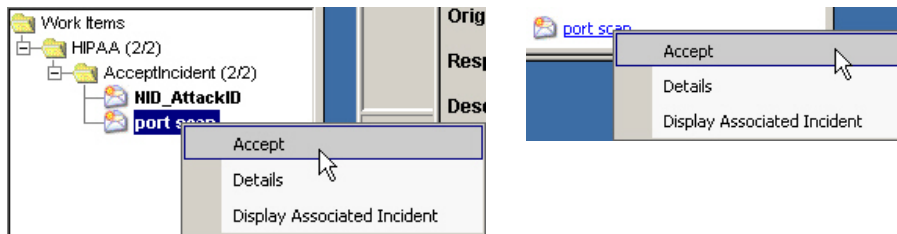
Il processo di interazione con un elemento di lavoro comprende tre passaggi:

- Accettazione di un elemento di lavoro
- Aggiornamento delle variabili nell'elemento di lavoro
- Completamento dell'elemento di lavoro

Accettazione di un elemento di lavoro

Un elemento di lavoro può essere assegnato a tutti gli utenti di un ruolo o solo a uno di essi. Per poter eseguire qualsiasi operazione sull'elemento di lavoro, l’utente deve prima accettarlo. In seguito a tale operazione, l’utente diventa proprietario dell’elemento di lavoro, che viene rimosso dall’elenco di lavoro di tutti gli altri utenti assegnati.

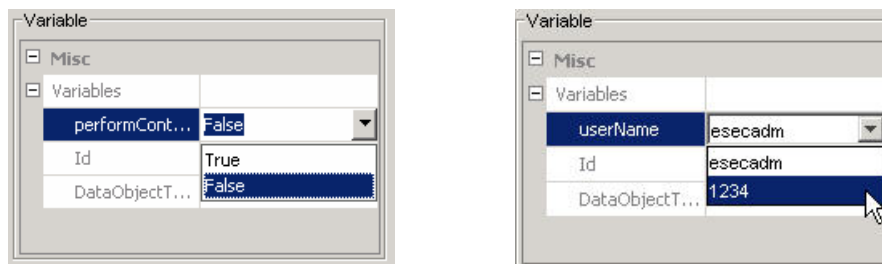
Accettazione di un elemento di lavoro

1. Nell’elenco di lavoro, è possibile fare clic con il pulsante destro del mouse su un elemento di lavoro ed eseguire le operazioni seguenti:

- Scegliere l’opzione Accetta (quando il processo è in una fase in cui tale operazione è consentita)
- Visualizzare, in alternativa, la finestra dei dettagli e fare clic sul pulsante Accetta.

Aggiornamento delle variabili nell'elemento di lavoro

Nel server iTRAC, gli elementi di lavoro sono utilizzati per ottenere informazioni dagli utenti nella forma di variabili degli elementi di lavoro al fine di individuare l’attività seguente di un processo. L’utente può accedere alle variabili solo dopo avere accettato l’elemento di lavoro.

In iTRAC sono supportate le variabili di sola lettura e quelle aggiornabili. Le prime consentono all’utente di conoscere informazioni quali lo stato di un’attività, l’ID di un caso e così via.

Le variabili aggiornabili sono utilizzate per accettare l’input degli utenti. Attualmente in iTRAC esistono due tipi di variabili aggiornabili, l’elenco degli utenti e l’elenco dei valori booleani.

Aggiornamento di variabili

1. Fare clic con il pulsante destro del mouse (o fare doppio clic) sull'elemento di lavoro per visualizzare la finestra di dialogo dei dettagli.

2. Solo le variabili aggiornabili possono essere modificate; le variabili di sola lettura non consentono modifiche.
3. Fare clic sulla casella combinata e selezionare il valore appropriato.

Completamento dell'elemento di lavoro

Il completamento dell'elemento di lavoro indica il completamento del task al server iTRAC. Le variabili aggiornabili dall'elemento di lavoro vengono elaborate dal server e ciò consente di passare all'attività successiva sulla base di determinati criteri. L'elemento di lavoro viene rimosso dall'elenco di lavoro dell'utente. Per poter essere completato, un elemento di lavoro deve essere prima accettato.

Completamento dell'elemento di lavoro

1. Fare clic con il pulsante destro del mouse (o fare doppio clic) sull'elemento di lavoro per visualizzare la finestra di dialogo dei dettagli.
2. Nella finestra di dialogo visualizzata, fare clic sul pulsante Completa.

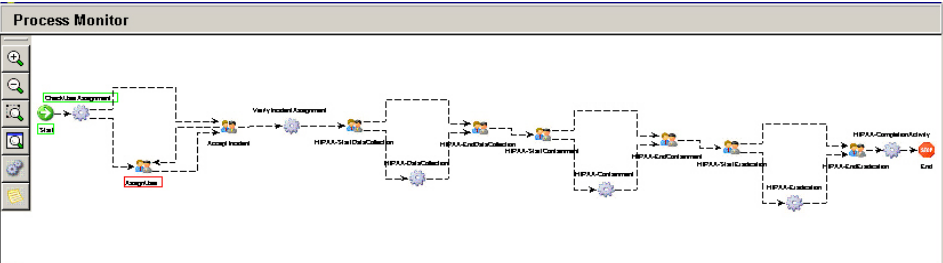
Gestione dei processi

La funzione Gestione processi consente di:

- Visualizzare lo stato del processo (Monitoraggio processo)
- Avviare il processo
- Terminare il processo

Monitoraggio processo

La funzione Monitoraggio processo consente di monitorare l'avanzamento di un processo. Durante lo svolgimento delle attività di un processo, l'utente può monitorare visivamente l'avanzamento del processo facendo clic sul pulsante Aggiorna. La funzione Monitoraggio processo inoltre fornisce un giornale di controllo di tutte le azioni svolte dal server iTRAC durante l'esecuzione del processo.

Le attività completate dal processo vengono visualizzate con un bordo verde mentre l'attività in esecuzione è contraddistinta da un bordo rosso.

Accesso al monitoraggio dei processi

1. Fare clic sulla scheda *iTRAC*.
2. Fare clic sul *pulsante Gestione opzioni visualizzazione* .
3. Fare doppio clic su una delle visualizzazioni di default o creare una nuova visualizzazione. Le visualizzazioni di default sono le seguenti:
   - Tutti i processi
   - Processi per caso
   - Processi per stato
4. In Gestione processi, evidenziare un processo e fare doppio clic su di esso.

Per impostare un'opzione in Gestione processi

1. Fare clic sulla scheda *iTRAC*.
2. Fare doppio clic su uno dei processi.
3. Fare clic sul pulsante Opzioni. In questa finestra è inoltre possibile impostare le opzioni seguenti:
   - Campi...
   - Raggruppa per...
   - Ordina...
   - Filtro...
   - Visualizzazione albero
4. Fare clic su *Applica* e su *Salva*.

   Se la visualizzazione ad albero è impostata su Stato (in esecuzione e non avviato) viene visualizzata la finestra seguente.

	State	IncidentId	LastUpdateTime	Description
Processes				
HIPAA				
SANS_Incident_Response				
running	running	104	2005.01.19 / 09:38:58 EST	SANS Incident H...
not_started	not_started	101	2005.01.18 / 08:52:59 EST	SANS Incident H...

Ready | Refresh | Options | Refreshed At: Fri Jan 21 13:04:40 EST 2005

Avvio o interruzione di un processo

Avvio o interruzione di un processo

1. Fare clic sulla scheda *iTRAC*.
2. Fare clic sul *pulsante Gestione opzioni visualizzazione* .
3. Fare doppio clic su una delle visualizzazioni di default o creare una nuova visualizzazione. Le visualizzazioni di default sono le seguenti:
   - Tutti i processi
   - Processi per caso
   - Processi per stato
4. In Gestione processi, evidenziare un processo, fare clic con il pulsante destro del mouse e selezionare *Avvia processo* o *Interrompi processo*.

Creazione di un'attività utilizzando il framework delle attività

Creazione di un'attività

1. Fare clic sulla scheda *iTRAC*.
2. Nella barra di spostamento fare clic su *Amministrazione iTRAC* > *Gestione attività*.
3. Fare clic con il pulsante destro del mouse e scegliere *Nuova attività*.
4. Selezionare una delle opzioni seguenti:

   - Attività comando del caso: consente di eseguire un comando specifico con o senza argomenti.

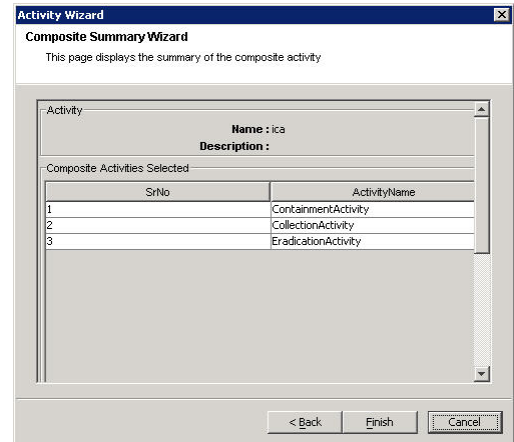
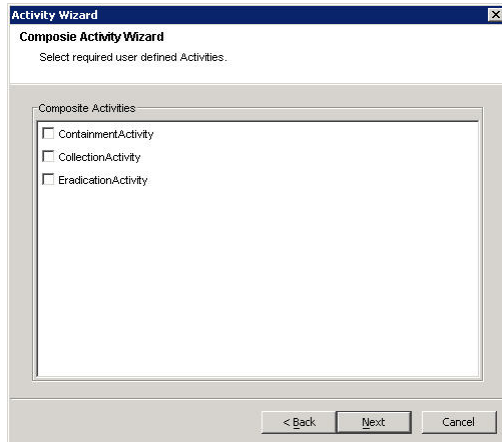
L’opzione Output caso fornisce gli argomenti seguenti:

- DIP
- SIP
- DIP:Porta
- SIP:Porta
- Caso
- RT1 (DeviceAttackName)
- Testo

L’opzione Personalizzato consente di specificare argomenti personalizzati.

Per questa attività è inoltre possibile inviare l’output tramite e-mail e/o allegarlo al caso.

- Attività interna del caso: consente di inviare tramite e-mail e/o allegare informazioni relative a:
  - Vulnerabilità (SIP o DIP)
  - Risorsa
  - Dati Advisor

- Attività composita del caso: consente di creare un’attività combinando una o più attività esistenti.

Modifica di un'attività

Modifica di un'attività

1. Fare clic sulla scheda *iTRAC*.
2. Nella barra di spostamento fare clic su *Amministrazione iTRAC* > *Gestione attività* > *Attività iTRAC*.
3. Fare doppio clic su un'attività iTRAC. Apportare le modifiche e fare clic su *OK*.

Importazione ed esportazione di un'attività

Le attività vengono esportate come file xml, che possono essere importati da un sistema a un altro.

Esportazione di un'attività

1. Fare clic sulla scheda *iTRAC*.
2. Nella barra di spostamento fare clic su *Amministrazione iTRAC* > *Gestione attività*.
3. Fare clic con il pulsante destro del mouse su *Attività iTRAC* > *Importa/esporta attività*.
4. Selezionare Esporta attività e fare clic sul pulsante *Esplora*.
5. Selezionare la cartella in cui si desidera salvare il file esportato.
6. Specificare un nome per il file e fare clic su *Esporta*.
7. Fare clic su *Avanti*.
8. Selezionare una o più attività da esportare.
9. Fare clic su *Avanti*, quindi su *Fine*.

Importazione di un’attività

1. Fare clic sulla scheda *iTRAC*.
2. Nella barra di spostamento fare clic su *Amministrazione iTRAC > Gestione attività*.
3. Fare clic con il pulsante destro del mouse su *Attività iTRAC > Importa/esporta attività*.
4. Selezionare Importa attività e fare clic sul pulsante *Esplora*.
5. Selezionare il file da importare. Fare clic su *Importa*.
6. Fare clic su *Avanti*.
7. Fare clic su *Avanti*, quindi su *Fine*.

6 Scheda Analisi

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Per utilizzare la scheda Analisi è necessario disporre dell'autorizzazione appropriata. Se questa autorizzazione non viene assegnata, non saranno disponibili neanche le altre autorizzazioni relative alle azioni eseguibili con questa scheda.

Descrizione

La scheda Analisi consente di eseguire rapporti cronologici. I rapporti cronologici e sulle vulnerabilità sono pubblicati su un server Web, vengono eseguiti direttamente sul database e sono visualizzati sulle schede Analisi e Advisor della barra di spostamento.

NOTA: Sentinel è integrato con Crystal Reports® per la generazione e la visualizzazione dei rapporti. L'amministratore deve configurare l'ubicazione del server Crystal Enterprise che pubblica i rapporti nella finestra Opzioni generali della scheda Amministratore. Nella finestra di navigazione è riportato un elenco dei rapporti disponibili.

Per eseguire i modelli dei rapporti, Crystal Reports Enterprise Edition deve essere installato e Sentinel Control Center deve essere configurato in modo da poter accedere al server. Per ulteriori informazioni, vedere *la Guida all'installazione di Sentinel™ 5*.

Sono inoltre forniti rapporti di esempio in formato pdf.

Primi dieci rapporti

Per eseguire uno qualsiasi dei primi dieci rapporti, è necessario che l'aggregazione sia abilitata e che in DAS_Binary.xml EventFileRedirectService sia impostato come attivo. Per informazioni su come abilitare l'aggregazione, vedere *il capitolo 10 "Gestione dati Sentinel" nella Guida dell'utente di Sentinel, nella sezione relativa alla scheda Rapporto dati*.

Abilitazione di EventFileRedirectService per i primi dieci rapporti di Sentinel

Abilitazione di EventFileRedirectService

1. Nel computer DAS, mediante l'editor di testo, aprire:

   Per UNIX:

   ```
   $ESEC_HOME/sentinel/config/das_binary.xml
   ```

   Per Windows:

   ```
   %ESEC_HOME%\sentinel\config\das_binary.xml
   ```

2. Per EventFileRedirectService, modificare lo stato su on.

```
<property name="status">on</property>
```

3. Per Windows, riavviare il servizio Sentinel. Per UNIX, riavviare il computer DAS.

Esecuzione di un rapporto da Crystal Reports

Per creare un rapporto da un modello di Crystal Reports

1. Fare clic sulla scheda *Analisi*.
2. Nella barra di spostamento *della scheda Analisi* fare clic su uno dei rapporti disponibili.

NOTA: Per eseguire uno qualsiasi dei primi dieci rapporti, è necessario che l'aggregazione sia abilitata e che in DAS_Binary.xml EventFileRedirectService sia impostato come attivo. Per informazioni su come abilitare l'aggregazione, vedere *il capitolo 10 "Gestione dati Sentinel" nella Guida dell'utente di Sentinel, nella sezione relativa alla scheda Rapporto dati*.

---

3. Fare clic su *Analisi* > *Crea rapporto* oppure fare clic sul pulsante *Crea rapporto*.

4. Completare le informazioni nel modello e fare clic su *Visualizza rapporto*. Il rapporto verrà visualizzato.

Esecuzione di un rapporto Interrogazione eventi

Per creare un rapporto Interrogazione eventi

1. Fare clic sulla scheda *Analisi*.
2. Nella barra di spostamento della scheda Analisi aprire la cartella Interrogazioni cronologiche.
3. Fare clic su *Interrogazione eventi*.
4. Fare clic su *Analisi* > *Crea rapporto* oppure fare clic sul pulsante *Crea rapporto*.

   Verrà visualizzata la finestra Interrogazione eventi.
5. Impostare quanto segue:
   - intervallo di tempo
   - filtro
   - livello di gravità
   - dimensioni batch, ovvero il numero di eventi da visualizzare (gli eventi saranno visualizzati in ordine cronologico, da quello meno recente a quello più recente)
6. Fare clic su *Aggiorna interrogazione*.
7. Per visualizzare il gruppo di eventi successivo, fare clic sul pulsante *Altro*.
8. Riorganizzare le colonne tramite la funzione di trascinamento e rilascio, quindi ordinarle facendo clic sull'intestazione della colonna.
9. Al termine, l'interrogazione sarà aggiunta all'elenco delle interrogazioni rapide nella barra di spostamento.

Esecuzione di un rapporto Eventi correlati

Per creare un rapporto Eventi correlati correlati

1. Fare clic sulla scheda *Analisi*.
2. Nella barra di spostamento della scheda Analisi aprire la cartella Interrogazioni cronologiche.
3. Fare clic su *Eventi correlati*.
4. Fare clic su *Analisi* > *Crea rapporto* oppure fare clic sul pulsante *Crea rapporto*.

   Verrà visualizzata la finestra del rapporto Eventi correlati.

5. Nel campo ID correlazione, immettere:
   - Numero ID evento, oppure
   - CorrelatedEventUUID (UUID eventi correlati)

NOTA: Il CorrelatedEventUUID è disponibile solo da una tabella eventi in tempo reale.

---

6. Per visualizzare il gruppo di eventi successivo, fare clic sul pulsante *Altro*.

7 Scheda Advisor

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Per utilizzare la scheda Advisor, è necessario disporre dell'apposita autorizzazione. Se questa autorizzazione non viene assegnata, non saranno disponibili neanche le altre autorizzazioni relative alle azioni eseguibili con questa scheda.

Advisor è un modulo facoltativo. Se non si possiede la relativa licenza, verrà visualizzata una schermata di notifica ogni volta che si fa clic sulla scheda Advisor.

Sentinel Advisor è sviluppato con tecnologia SecurityNexus. Advisor offre funzioni di analisi in tempo reale delle vulnerabilità aziendali, suggerimenti, indicazioni e procedure per l'adozione delle misure di risposta appropriate. In Advisor è incluso un riferimento incrociato tra le firme degli attacchi IDS in tempo reale e la Knowledge Base dell'applicazione relativa alle vulnerabilità. Per ulteriori informazioni, visitare il sito all'indirizzo http://www.esecurity.net/Software/Products/Advisor.asp.

Il feed di dati di Advisor è suddiviso in due parti:

- Dati degli avvisi: informazioni relative a vulnerabilità e minacce note della sicurezza
- Dati degli attacchi: normalizzazione delle firme di rilevazione delle intrusioni e plug-in di scansione delle vulnerabilità

NOTA: La funzione del tasto destro del mouse su un evento (con il campo rt1 popolato) non sarà disponibile per i dati di Advisor nella fase di installazione e fino al feed di dati iniziale da parte di SecurityNexus.

Esecuzione dei rapporti di Advisor

Per creare un rapporto di Advisor

1. Fare clic sulla scheda Advisor.
2. Nella barra di navigazione di Advisor, fare clic su un modello di rapporto.
3. Fare clic su *Advisor* > *Crea rapporto*.
4. Completare le informazioni nel modello e fare clic su *Visualizza rapporto*.

Installazione autonoma: Aggiornamento manuale di Advisor

Aggiornamento manuale del feed di dati di Advisor

1. Accedere all’URL //advisor.esecurityinc.com/advisordata/.
2. Immettere nome utente e password.

3. Accedere alle cartelle degli attacchi e degli avvisi relativi all'ultimo mese, quindi scaricare i file zip.
4. Posizionare i nuovi file (in formato zip) dei dati di feed relativi ad avvisi e attacchi nel computer in uso.

NOTA: Non posizionare i file zip direttamente nelle directory degli attacchi e degli avvisi.

---

5. Decomprimere i file zip contenenti i feed di dati per gli attacchi in:

   Per Windows:

   ```
   <ubicazione specificata durante l'installazione dei
      file di dati di Advisor>\attack
   ```

   oppure

   Per UNIX:

   ```
   <ubicazione specificata durante l'installazione dei
      file di dati di Advisor>/attack
   ```

6. Decomprimere i file zip contenenti i feed di dati per gli avvisi in:

   Per Windows:

   ```
   <ubicazione specificata durante l'installazione dei
      file di dati di Advisor>\alert
   ```

   oppure

   Per UNIX:

   ```
   <ubicazione specificata durante l'installazione dei
      file di dati di Advisor>/alert
   ```

7. Passare a:

   Per Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

   Per UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

8. Eseguire il comando seguente:

   Per Windows:

   ```
   advisor.bat
   ```

   Per UNIX:

   ```
   ./advisor.sh
   ```

NOTA: Advisor.sh e advisor.bat determinano l'aggiornamento del database seguito dall'eliminazione dei file degli attacchi e degli avvisi che erano stati decompressi nelle rispettive directory.

Download Internet diretto: Aggiornamento manuale di Advisor

Aggiornamento manuale del feed di dati di Advisor

1. Passare a:

   Per Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

   Per UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

2. Eseguire il comando seguente:

   Per Windows:

   ```
   advisor.bat
   ```

   Per UNIX:

   ```
   ./advisor.sh
   ```

NOTA: Advisor.sh e advisor.bat determinano l'aggiornamento del database seguito dall'eliminazione dei file degli attacchi e degli avvisi che erano stati decompressi nelle rispettive directory.

Modifica della password e della configurazione e-mail del server Advisor

Modifica della password del server Advisor (modalità autonoma)

Procedura che non può essere eseguita in modalità autonoma.

Modifica della password del server Advisor (download diretto)

Per modificare la password del server Advisor (download diretto)

1. Richiedere la modifica della password al supporto tecnico Novell.
2. Una volta ricevuta la notifica da parte di Novell dell'avvenuta modifica della password, eseguire il login come utente esecadm per UNIX oppure come utente con diritti di amministrazione per Windows.
3. Passare alla directory:

   Per UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

   Per Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

4. Immettere i comandi seguenti:

   Per UNIX:

```
./adv_change_passwd.sh <passwordprecedente>
   <nuovapassword>
```

   Per Windows:

```
adv_change_passwd.bat <passwordprecedente>
   <nuovapassword>
```

Modifica della configurazione e-mail del server Advisor

Per modificare la configurazione e-mail del server Advisor

1. Per UNIX eseguire il login come utente esecadm oppure per Windows eseguire il login come utente con diritti di amministrazione.
2. Passare alla directory:

   Per UNIX:

```
$ESEC_HOME/sentinel/config
```

   Per Windows:

```
%ESEC_HOME%\sentinel\config
```

3. Utilizzando un editor di testo, aprire i file alertcontainer.xml e alertcontainer.xml. Apportare le modifiche desiderate nell'area evidenziata in grigio.

```
<property
   name="advisor.mail.from">daNOME@dominio.com</proper
   ty>

<property
   name="advisor.mailto.list">aNOME@dominio.com</prope
   rty>
```

NOTA: Per immettere più indirizzi di e-mail, aggiungere una virgola tra gli indirizzi, senza alcuno spazio aggiuntivo.

Modifica dell'orario del feed di dati

Per default, il feed di dati viene eseguito:

- Ogni sei ore: alle ore 01.00, 07.00, 13.00 e 19.00
- Ogni dodici ore: alle ore 02.00 e 14.00

Per modificare tali impostazioni

1. Eseguire il login al computer che esegue Advisor (per UNIX eseguire il login come utente esecadm).
2. Per modificare gli orari di esecuzione del feed di dati:

   Per UNIX: utilizzare il comando 'crontab'

   Per Windows: utilizzare il comando 'at'

Scheda Servizi di raccolta

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Per utilizzare la scheda Servizi di raccolta è necessario disporre dell'autorizzazione appropriata. La scheda Servizi di raccolta consente una funzionalità Wizard limitata. Per una funzionalità Wizard completa, utilizzare il Generatore servizi di raccolta. La scheda Servizi di raccolta consente di:

- monitorare un host Wizard
- monitorare un Servizio di raccolta
- avviare e arrestare un servizio di raccolta (Gestione servizi di raccolta) per un host specifico

Layout

Nel pannello di sinistra della scheda Servizi di raccolta è riportato un albero delle visualizzazioni. Per default, la radice dell'albero ha due figli: Visualizzazioni Gestione servizi di raccolta e Visualizzazione servizio di raccolta. Nel pannello di destra le visualizzazioni sono organizzate in tabelle. A ciascuna visualizzazione del pannello di destra è associata una voce nell'albero di sinistra.

Nel pannello di destra sono riportate quattro visualizzazioni:

- Visualizzazione servizio di raccolta
  - Gestione visualizzazione servizio di raccolta
- Visualizzazione Gestione servizi di raccolta
  - Gestione visualizzazione Gestione servizi di raccolta

In Visualizzazione servizio di raccolta sono visualizzate informazioni sui Servizi di raccolta, mentre in Visualizzazione Gestione servizi di raccolta sono visualizzate informazioni sulle istanze di Gestione servizi di raccolta. Ogni visualizzazione è visualizzata come una tabella ad albero: l'oggetto è raggruppato in base a uno o più attributi. La configurazione della visualizzazione può essere modificata. È infatti possibile modificare le opzioni di una visualizzazione e aggiungere nuovi tipi di visualizzazione. La configurazione della visualizzazione è visualizzata in Gestione visualizzazioni (Gestione visualizzazione servizio di raccolta oppure in Gestione visualizzazione Gestione servizi di raccolta).

Quando la scheda viene visualizzata per la prima volta, l'albero nel pannello di sinistra contiene le due gestioni di visualizzazione e Gestione visualizzazione servizio di raccolta viene visualizzato nel pannello di destra.

Gestione visualizzazione servizio di raccolta ha 3 opzioni di visualizzazione pre-configurate per default ed è possibile crearne di nuove. Le opzioni disponibili consentono di visualizzare tutti i servizi di raccolta, i servizi di raccolta per manager e i servizi di raccolta per stato. tutti i servizi di raccolta, i servizi di raccolta per manager e i servizi di raccolta per stato.

Nella visualizzazione di tutti i servizi di raccolta sono visualizzati tutti i Servizi di raccolta raggruppati in base alla gestione in cui sono eseguiti.

Nella visualizzazione dei servizi di raccolta per manager sono raggruppati tutti i Servizi di raccolta in base al manager e successivamente in base al relativo stato (attivo oppure disattivo) all'interno di ogni manager.

Nella visualizzazione dei servizi di raccolta per stato sono raggruppati tutti i Servizi di raccolta in base allo stato (Attivo oppure Disattivo) e successivamente in base alla gestione.

La visualizzazione di default nelle istanze di Gestione servizi di raccolta è la visualizzazione di tutti i manager, nella quale sono visualizzate tutte le gestioni attive del Servizio di raccolta presenti nel sistema senza alcun raggruppamento.

Monitoraggio di un servizio di raccolta

Nella finestra di host Wizard è possibile monitorare per default quanto segue:

Gestione visualizzazione Gestione servizi di raccolta

- Ora inizio — Orario in cui è stato avviato Gestione servizi di raccolta, espresso in gg/mm/aa hh:mm:ss e fuso orario
- Tempo di attività — Intervallo di tempo in cui Gestione servizi di raccolta è stato in esecuzione, espresso in giorni, ore, minuti e secondi.
- Totale eventi ricevuti — Numero di eventi ricevuti da tutti i Servizi di raccolta in base a Gestione servizi di raccolta dall'avvio dello stesso.
- Frequenza eventi ricevuti — Frequenza media di eventi al secondo ricevuta da Gestione servizi di raccolta nell'ultimo minuto.

Gestione visualizzazione servizio di raccolta

- Stato — Attivo o Disattivo
- Frequenza eventi ricevuti — Frequenza media di eventi al secondo ricevuta dalla porta del servizio di raccolta nell'ultimo minuto.

- Totale eventi ricevuti — Numero di eventi ricevuti dalla porta del servizio di raccolta dall'avvio dello stesso.
- Tempo di attività — Intervallo di tempo in cui la porta del servizio di raccolta è stata in esecuzione, espresso in ore, minuti e secondi.

È possibile creare visualizzazioni personalizzate con un numero maggiore o minore di campi.

Monitoraggio di un host Wizard

Monitoraggio di un host Wizard

1. Fare clic sulla scheda Servizi di raccolta.
2. Fare clic su *Gestione visualizzazione servizio di raccolta* .
3. Selezionare un'opzione di visualizzazione facendo doppio clic su una delle visualizzazioni o creare una nuova visualizzazione. Verrà visualizzata la finestra di host Wizard.

Collector View Manager

Nome	Campi	Raggruppa per	Ordina	Filtro
ALL COLLECTORS	Stato,Frequenza eventi ricevuti...	Nome manager:(Ascending)	None	Off
COLLECTORS BY MANAGER	EventsReceivedRate,EventsRe...	ManagerName(Ascending),Stat...	None	Off
COLLECTORS BY STATUS	Stato,Frequenza eventi ricevuti...	Stato(Ascending)...	None	Off

Pronto — Aggiorna — Applica — Aggiungi visualizzazione

Creazione di una Visualizzazione servizio di raccolta

Creazione di una Visualizzazione servizio di raccolta

1. Fare clic sulla scheda *Servizi di raccolta*.
2. Aprire Gestione *visualizzazione servizio di raccolta*.

3. Per creare una nuova visualizzazione, fare clic sul pulsante *Aggiungi visualizzazione*.
   - Immettere un valore nel campo Nome opzione.
   - Per determinare i campi da visualizzare, fare clic sul pulsante *Campi*.
   - Per raggruppare titoli diversi, fare clic sul pulsante *Raggruppa per*.
   - Per ordinare in base al titolo, fare clic sul pulsante *Ordina*.
   - Per applicare un filtro, fare clic sul pulsante *Filtro*.

   La visualizzazione seguente è organizzata in funzione del nome della porta e con il gruppo impostato sull'UUID del manager.

Modifica di una Visualizzazione servizio di raccolta

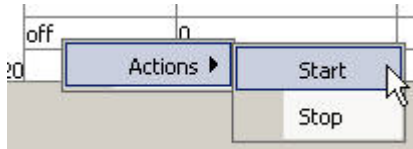
Modifica di una Visualizzazione servizio di raccolta

1. Aprire Gestione visualizzazione servizio di raccolta.
2. Fare doppio clic su uno dei nomi.
3. Fare clic su *Opzioni*. In questa finestra è inoltre possibile impostare le opzioni seguenti:
   - Campi...
   - Raggruppa per...
   - Ordina...
   - Filtro...
   - Visualizzazione albero
4. Fare clic su *Applica* e su *Salva*.

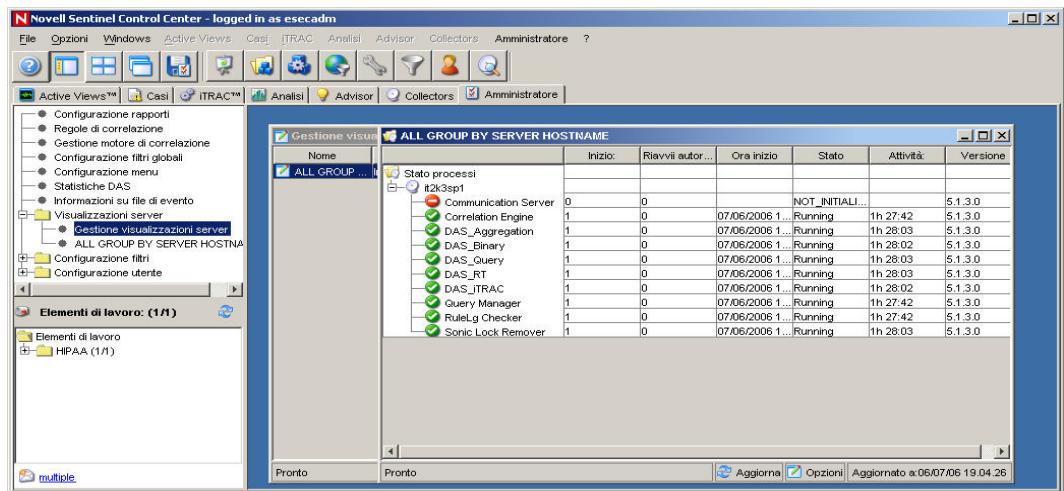
   Nella visualizzazione seguente la visualizzazione ad albero è impostata sull'UUID del manager.

Arresto/Avvio/Dettagli dei Servizi di raccolta

Arresto/Avvio dei Servizi di raccolta

1. Fare clic sulla *scheda Servizi di raccolta*.
2. Aprire Gestione visualizzazione servizio di raccolta.
3. Per arrestare/avviare/mostrare i dettagli di un singolo Servizio di raccolta, fare clic con il pulsante destro del mouse su un Servizio di raccolta, quindi su *Azioni* e in seguito su *Avvia o Arresta*.

Scheda Amministratore

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Per utilizzare questa funzione, è necessario disporre dell'autorizzazione appropriata. Se questa autorizzazione non viene assegnata, non saranno disponibili neanche le altre autorizzazioni relative alle azioni eseguibili con questa scheda.

Scheda Amministratore: Descrizione

La scheda Amministratore consente di accedere a quanto segue:

- Opzioni di configurazione dei rapporti di Analisi e Advisor
- Manage filters
- Utilizzo delle regole di correlazione di Sentinel
- Configurazione della finestra Configurazione menu
- Statistiche DAS
- Informazioni sul file di evento
- Visualizzazioni server
- Configurazione di un conto utente

Opzioni di configurazione dei rapporti di Analisi e Advisor

Per configurare l'URL dei rapporti di Analisi e Advisor

1. Fare clic sulla scheda *Amministratore*.
2. Nella barra di *spostamento fare* clic su *Configurazione rapporti*.

3. Nella finestra *Configurazione rapporti* fare clic su *Modifica*.
   - Immettere l'URL di Crystal Enterprise Server nel campo URL analisi, quindi fare clic su Aggiorna.

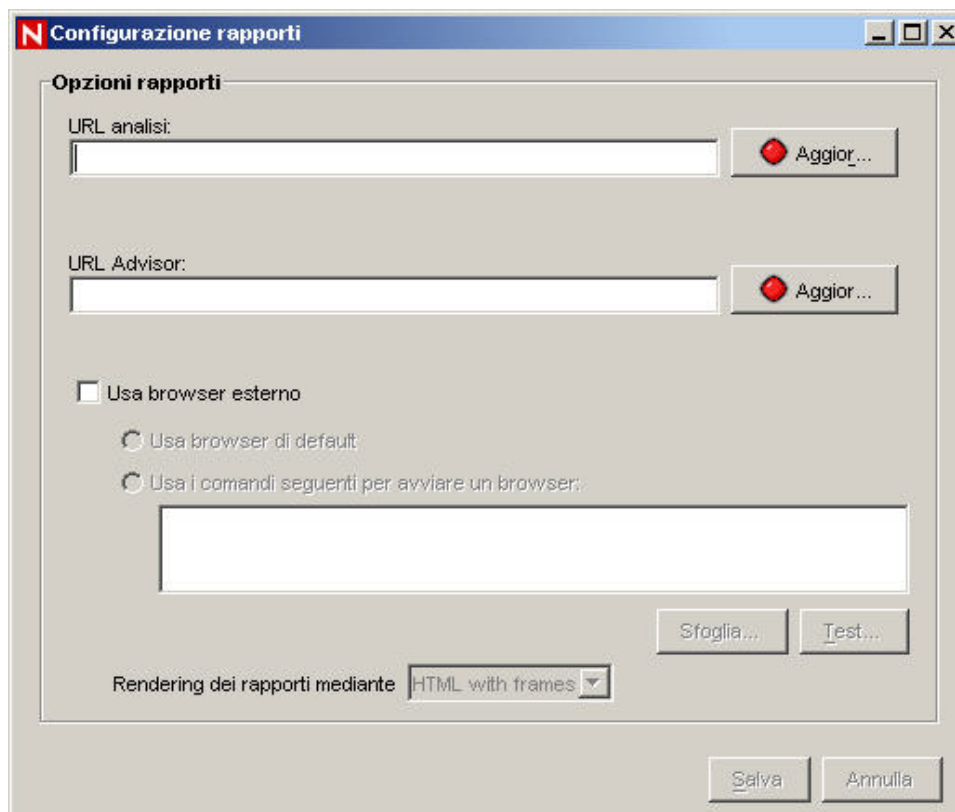
     ```
     http://<IP>/GetReports.asp?APS=<IP>&user=Guest&passwor
        d=&tab=Analysis
     ```

NOTA: <IP> è l'indirizzo IP di Crystal Enterprise Server.

   - Immettere l'URL di Crystal Enterprise Server nel campo URL Advisor, quindi fare clic su *Aggiorna*.

     ```
     http://<IP>/GetReports.asp?APS=<IP>&user=Guest&passwor
        d=&tab=Advisor
     ```

NOTA: <IP> è l'indirizzo IP di Crystal Enterprise Server.

Per ulteriori informazioni, vedere *la Guida all'installazione*.

L'opzione del browser esterno consente di utilizzare il browser di default oppure un altro browser. Se si utilizza un browser diverso da quello di default, la riga di comando deve essere seguita da un parametro %URL%. Ad esempio:

```
C:\Programmi\Internet Explorer\IEXPLORE.EXE %URL%
```

4. Attendere che il pulsante Aggiorna diventi verde, quindi fare clic su Salva. Sarà necessario eseguire il logout da Sentinel Control Center, quindi eseguire nuovamente il login.

Utilizzo delle regole di correlazione di Sentinel

Grazie alla correlazione sono disponibili nuove funzioni di gestione degli eventi di sicurezza, le quali consentono di automatizzare l'analisi del flusso di eventi in ingresso per individuare eventuali schemi di interesse. La correlazione consente di definire regole per l'identificazione di minacce critiche e modelli di attacco complessi, al fine di poter stabilire una priorità per gli eventi, nonché reagire e gestire i casi in modo efficace.

Le regole di correlazione sono raggruppate in modo logico nelle cartelle delle regole. Tale raggruppamento consente di avere un unico insieme di regole che viene eseguito durante l'orario di lavoro, di notte o nel fine settimana. In pratica, consente di avere un insieme di regole che controlla diverse attività in base all'orario.

Ad esempio, è possibile abilitare alle ore 8 dei giorni compresi tra il lunedì e il venerdì tutte le regole di correlazione diurne oppure disabilitare tutte le regole di correlazione notturne in un'unica operazione. Se non è quindi necessario raggruppare le regole di correlazione in cartelle di regole diverse, basterà un'unica cartella dove posizionare tutte le regole di correlazione.

Non esiste un limite al numero di persone che possono accedere alle Regole di correlazione. Se più utenti stanno modificando la stessa regola, l'ultima persona che eseguirà il salvataggio sovrascriverà tutte le modifiche precedenti.

In questa sezione vengono trattati gli argomenti seguenti:

- Regole e cartelle delle regole
- Tipi di regole di correlazione
- Distribuzione delle regole del motore di correlazione
- Importazione ed esportazione delle regole di correlazione
- Ruolo del database nella memorizzazione delle regole di correlazione
- Condizioni logiche

NOTA: Non è possibile eseguire la correlazione su un valore nullo (vuoto).

Regole e cartelle delle regole

In questa sezione viene definita la relazione tra le cartelle delle regole e le regole stesse. Le cartelle delle regole e le regole sono visualizzate in ordine gerarchico nella finestra Regole di correlazione.

- Ogni cartella può contenere più regole o nessuna regola
- Il numero di cartelle e di regole dipende solo dallo spazio su disco (memoria) disponibile
- Facendo doppio clic su una cartella delle regole viene visualizzato l'editor delle regole per il tipo di regola di correlazione corrispondente
- I nomi delle cartelle e delle regole possono avere una lunghezza massima di 255 caratteri
- Le descrizioni delle cartelle e delle regole possono avere una lunghezza massima di 1024 caratteri

Tipi di regole di correlazione

Durante la definizione delle regole, è possibile scegliere tra quattro tipi di regole di correlazione, ovvero:

- Watchlist
- Correlazione base

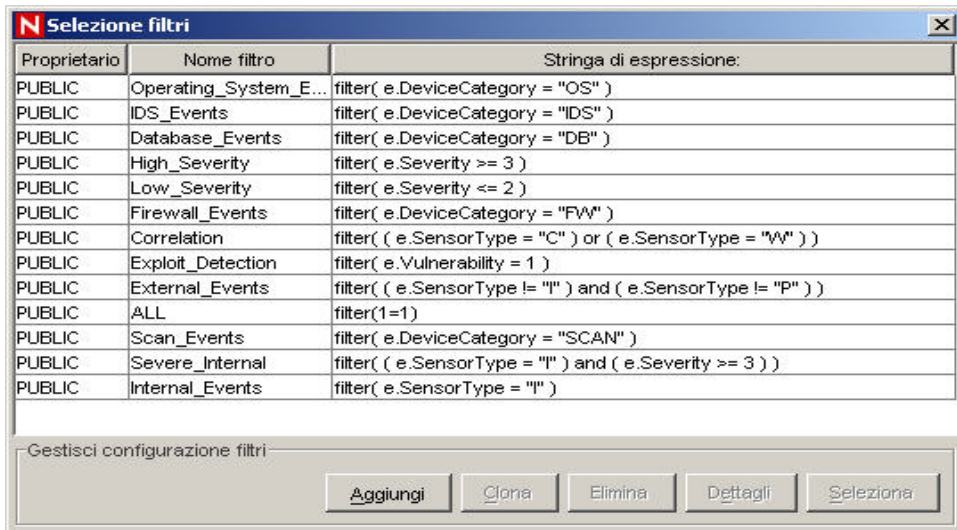
- Correlazione avanzata
- RuleLg in formato libero

ATTENZIONE: Prima di utilizzare questo tipo di regola di correlazione, è consigliabile acquisire ulteriori informazioni sul linguaggio di definizione delle regole di correlazione RuleLg. Inoltre, se è stato rinominato un tag, non utilizzare il nome originale per la creazione di una regola di correlazione con RuleLg.

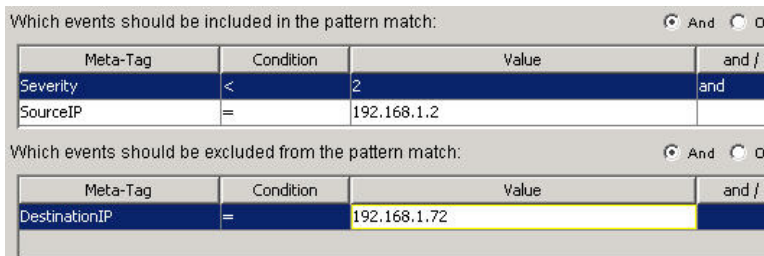
Watchlist

È possibile scegliere fra quattro diversi tipi di filtro, ovvero:

- Consenti tutto: ammette tutti gli eventi.
- Schema: qualsiasi espressione regolare con sintassi analoga a grep.
- Gestione filtri: elenco a discesa che consente di selezionare o creare un nuovo filtro di Gestione filtri.

Proprietario	Nome filtro	Stringa di espressione:
PUBLIC	Operating_System_E...	filter(e.DeviceCategory = "OS")
PUBLIC	IDS_Events	filter(e.DeviceCategory = "IDS")
PUBLIC	Database_Events	filter(e.DeviceCategory = "DB")
PUBLIC	High_Severity	filter(e.Severity >= 3)
PUBLIC	Low_Severity	filter(e.Severity <= 2)
PUBLIC	Firewall_Events	filter(e.DeviceCategory = "FW")
PUBLIC	Correlation	filter((e.SensorType = "C") or (e.SensorType = "W"))
PUBLIC	Exploit_Detection	filter(e.Vulnerability = 1)
PUBLIC	External_Events	filter((e.SensorType != "I") and (e.SensorType != "P"))
PUBLIC	ALL	filter(1=1)
PUBLIC	Scan_Events	filter(e.DeviceCategory = "SCAN")
PUBLIC	Severe_Internal	filter((e.SensorType = "I") and (e.Severity >= 3))
PUBLIC	Internal_Events	filter(e.SensorType = "I")

- Generatore: consente di creare criteri di inclusione ed esclusione degli eventi in base all'algebra booleana. Sono disponibili due riquadri (inclusione ed esclusione). Immettere i valori nei riquadri. Ad esempio:

Meta-Tag	Condition	Value	and / o
Severity	<	2	and
SourceIP	=	192.168.1.2	

Meta-Tag	Condition	Value	and / o
DestinationIP	=	192.168.1.72	

Correlazione base

È possibile scegliere fra quattro diversi tipi di filtro, ovvero:

- Consenti tutto: ammette tutti gli eventi.
- Schema: qualsiasi espressione regolare con sintassi analoga a grep.

- Gestione filtri: elenco a discesa che consente di selezionare o creare un nuovo filtro di Gestione filtri.
- Generatore: consente di creare criteri di inclusione ed esclusione degli eventi in base all'algebra booleana.

Questa regola consente di conteggiare il numero di volte in base al quale alcune condizioni vengono soddisfatte in un intervallo di tempo specifico.

Una regola di correlazione base consente, ad esempio, di cercare lo stesso indirizzo IP di origine segnalato cinque volte in cinque minuti, anche se gli eventi si riferiscono a dispositivi differenti, come un sistema di rilevazione delle intrusioni (IDS) e un firewall.

Correlazione avanzata

È possibile scegliere fra quattro diversi tipi di filtro, ovvero:

- Consenti tutto: ammette tutti gli eventi.
- Schema: qualsiasi espressione regolare con sintassi analoga a grep.
- Gestione filtri: elenco a discesa che consente di selezionare o creare un nuovo filtro di Gestione filtri.
- Generatore: consente di creare criteri di inclusione ed esclusione degli eventi in base all'algebra booleana.

Questa regola consente di:

- Conteggiare il numero di volte in base al quale alcune condizioni vengono soddisfatte in un intervallo di tempo specifico.
- Incorporare tutte le funzioni della regola di correlazione semplice nonché valutare gli eventi in base ad alcuni eventi precedenti.

Una regola di correlazione avanzata consente, ad esempio, di cercare eventi provenienti dallo stesso indirizzo IP di origine e diretti allo stesso indirizzo IP di destinazione, che abbiano lo stesso nome e che si verifichino sia all'interno che all'esterno di un firewall, ad indicare un attacco realizzato attraverso il firewall.

Correlazione RuleLg in formato libero

Il linguaggio di definizione delle regole di correlazione RuleLg consente di assumere il controllo completo ai fini della definizione delle regole di correlazione. Prima di utilizzare questo tipo di regola di correlazione, è consigliabile acquisire ulteriori informazioni sul linguaggio di definizione delle regole di correlazione RuleLg.

Distribuzione delle regole del motore di correlazione

Per utilizzare questa funzione, è necessario disporre dell'autorizzazione utente di avvio e arresto del motore di correlazione. Il motore di correlazione è attivato o disattivato. Lo stato attuale del motore è visualizzato nell'icona.

- Attivato -
- Disattivato -

Quando il motore di correlazione è attivato, vengono elaborate nuove cartelle di regole di correlazione.

Quando è disattivato, tutti i dati della memoria vengono preservati e non vengono generati nuovi eventi di correlazione. Questo stato corrisponde alla disattivazione di tutte le cartelle delle regole. La disattivazione del motore di correlazione non ha alcun effetto sulle altre parti

del sistema. Gli eventi in ingresso vengono comunque elaborati e il database di Sentinel continua a essere compilato.

Importazione ed esportazione delle regole di correlazione

La funzione di esportazione di Sentinel consente di creare ed esportare regole di correlazione predefinite, che possono essere importate nel sistema in uso dall'utente. Questi documenti XML sono formattati in modo specifico per il motore di correlazione. Le regole predefinite vengono generate da Sentinel e sono disponibili nel portale del servizio clienti all'indirizzo http://www.esecurityinc.com (in lingua inglese).

La possibilità di esportare le regole in formato XML è utile quando si necessita di assistenza da parte di Novell per la risoluzione di problemi legati alle regole di correlazione, nonché quando si possiedono due ambienti di Sentinel: uno di sviluppo e uno di produzione. È possibile eseguire il test delle regole di correlazione nell'ambiente di sviluppo ed esportarle successivamente nell'ambiente di produzione. Le regole di correlazione vengono esportate in formato .crf.

Ruolo del database nella memorizzazione delle regole di correlazione

Quando si attiva il motore di correlazione (processo del server Sentinel) in Sentinel Control Center, vengono richieste le regole e informazioni di distribuzione dal database. Le regole di correlazione, modificate e poi salvate, vengono inviate al database per essere memorizzate. Le modifiche apportate non verranno visualizzate nel motore di correlazione, a meno che una delle seguenti condizioni venga soddisfatta:

- La regola distribuita viene disabilitata, quindi riabilitata.
- La regola è appena stata distribuita.

Le regole di distribuzione, modificate e poi salvate, vengono inviate al database per essere memorizzate e al motore di correlazione per essere utilizzate.

Condizioni logiche delle regole di correlazione

Di seguito sono riportate le condizioni logiche che vengono utilizzate quando si creano regole di correlazione. Per ulteriori informazioni sui tag META, vedere *la Guida di riferimento dell'utente*.

Condizione	**Tipo di campo**	**Descrizione**
=	di tipo numerico stringa	Il contenuto del tag META selezionato è uguale al valore immesso.
!=	di tipo numerico stringa	Il contenuto del tag META selezionato è diverso rispetto al valore immesso.
<	di tipo numerico	Il contenuto della proprietà selezionata è minore del valore immesso.
>	di tipo numerico	Il contenuto del tag META selezionato è maggiore del valore immesso.
<=	di tipo numerico	Il contenuto del tag META selezionato è minore o uguale al valore immesso.
>=	di tipo numerico	Il contenuto del tag META selezionato è maggiore o uguale al valore immesso.

Condizione	Tipo di campo	Descrizione
=Tag Meta	di tipo numerico stringa	Il contenuto del tag META selezionato dall'elenco a discesa a sinistra è uguale al contenuto del tag META selezionato a destra dell'espressione.
!=Tag Meta	di tipo numerico stringa	Il contenuto del tag META selezionato dall'elenco a discesa a sinistra è diverso rispetto al contenuto del tag META selezionato a destra dell'espressione.
<Tag Meta	di tipo numerico	Il contenuto del tag META selezionato dall'elenco a discesa a sinistra è minore del contenuto del tag META selezionato a destra dell'espressione.
>Tag Meta	di tipo numerico	Il contenuto del tag META selezionato dall'elenco a discesa a sinistra è maggiore del contenuto del tag META selezionato a destra dell'espressione.
<=Tag Meta	di tipo numerico	Il contenuto del tag META selezionato dall'elenco a discesa a sinistra è minore o uguale al contenuto del tag META selezionato a destra dell'espressione.
>=Tag Meta	di tipo numerico	Il contenuto del tag META selezionato dall'elenco a discesa a sinistra è maggiore o uguale al contenuto del tag META selezionato a destra dell'espressione.
=Regex	di tipo numerico stringa	Utilizzare il punto (.) e l'asterisco (*) nella stringa per indicare il valore.
Sottorete	di tipo numerico stringa	L'operazione della sottorete sarà corrispondente se l'indirizzo IP di paragone appartiene alla stessa sottorete specificata nell'operazione corrispondente.

Apertura della finestra Regole di correlazione

In questa sezione vengono descritte le funzioni della finestra Regole di correlazione

- Nuova cartella: consente di creare una nuova cartella delle regole
- Nuova regola: consente di creare una regola per una cartella delle regole
- Copia regola: consente di modificare le regole o le relative cartelle copiate, pur mantenendo una copia della regola o della relativa cartella di origine
- Elimina una cartella delle regole o una regola: dopo aver confermato l'eliminazione, non sarà più possibile recuperare la regola o la relativa cartella eliminata
- Rinomina: consente di rinominare una regola o una cartella delle regole
- Importa cartella delle regole: si aprirà la finestra di un browser
- Esporta cartella delle regole: si aprirà la finestra di un browser e la cartella delle regole verrà esportata in formato XML
- Modifica: consente di modificare e visualizzare le proprietà di regole e cartelle in anteprima

Per aprire la finestra Regole di correlazione

1. Fare clic sulla scheda *Amministratore*.
2. Nella barra di *spostamento fare* clic su *Regole di correlazione*.

Copia e creazione di una regola o di una cartella delle regole

Per creare una cartella delle regole

1. Aprire la finestra Regole di correlazione.
2. Selezionare la cartella superiore che dovrà contenere la nuova cartella.
3. Fare clic con il pulsante destro del mouse, quindi scegliere *Nuova cartella*.
4. Digitare il nome della cartella delle regole. Il nome, che prevede la distinzione tra maiuscole e minuscole, non deve essere superiore a 255 caratteri né contenere punti.
5. Digitare una descrizione della regola (facoltativo). La descrizione non deve essere superiore a 1024 caratteri.
6. Fare clic su *OK*.

Per creare una regola

1. Selezionare la cartella superiore che dovrà contenere la nuova regola.
2. Fare clic con il pulsante destro del mouse, quindi scegliere *Nuova regola*.
3. Si aprirà la procedura guidata per la creazione delle regole. Selezionare uno dei tipi di regola seguenti:
   - Watchlist
   - Correlazione base
   - Correlazione avanzata
   - Formato libero

   NOTA: Per ulteriori informazioni sui tipi di regole, vedere la sezione Tipi di regole di correlazione.
4. Fare clic su *Fine*.

Eliminazione delle regole di correlazione o della relativa cartella

Per eliminare le regole di correlazione o la relativa cartella

1. Aprire la finestra Regole di correlazione.
2. Selezionare la regola o la cartella delle regole che si intende eliminare.
3. Fare clic con il pulsante destro del mouse, quindi scegliere *Elimina*.
4. Verrà visualizzata una finestra di conferma.
   - Premendo Sì, la cartella delle regole verrà eliminata. Ciò comporta l'eliminazione di tutte le regole in essa contenute. Questa operazione è irreversibile.
   - Premendo No, si tornerà alla finestra Regole di correlazione.

Importazione ed esportazione di una cartella delle regole di correlazione

Per importare o esportare una cartella delle regole di correlazione

1. Aprire la finestra Regole di correlazione.
2. Selezionare una cartella delle regole.
3. Fare clic con il pulsante destro del mouse, *quindi scegliere Importa cartella delle regole oppure Esporta cartella delle regole*.

- Nel caso dell'importazione, verrà avviato un browser di file. Individuare la cartella delle regole da importare, quindi fare clic su *OK*.
- Nel caso dell'esportazione, verrà avviato un browser di file. Individuare il dispositivo di destinazione sul quale scrivere la cartella delle regole, quindi fare clic su *OK*. La cartella verrà esportata in formato CRF.

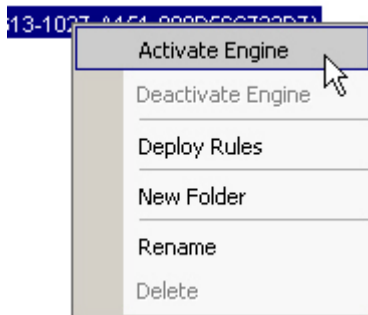
Esecuzione di modifiche nella finestra Regole di correlazione

Per eseguire modifiche nella finestra Regole di correlazione

1. Aprire la finestra Regole di correlazione.
2. Fare clic con il pulsante destro del mouse, quindi scegliere *Modifica*.
3. Modificare la regola, quindi fare clic su *Fine*.

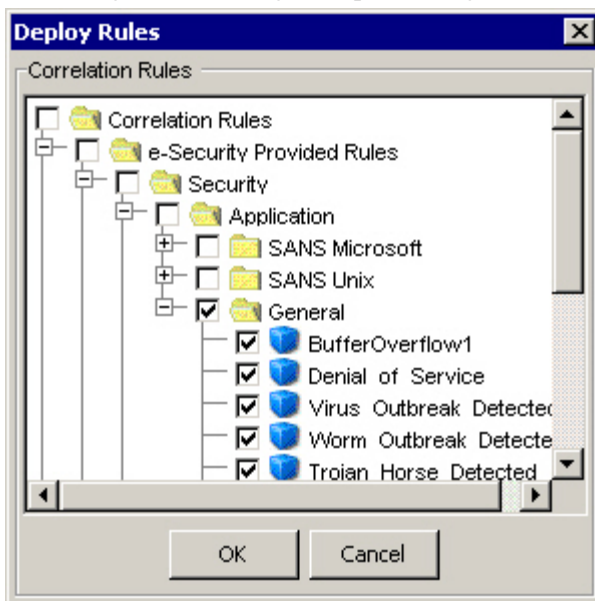
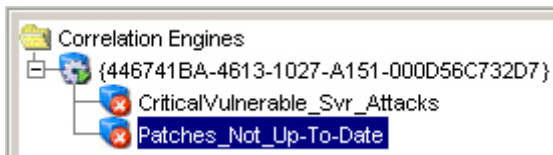
Attivazione o disattivazione del motore di correlazione

Per attivare o disattivare il motore di correlazione

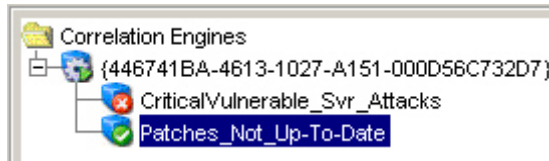
1. Aprire la finestra Gestione motore di correlazione.
2. Selezionare un motore di correlazione. *Fare clic con il pulsante destro del mouse, quindi scegliere Attiva motore oppure Disattiva motore*.

Distribuzione delle regole di correlazione

Per distribuire le regole di correlazione

1. Aprire la finestra Gestione motore di correlazione.

2. Fare clic con il tasto destro del mouse su qualsiasi cartella nella finestra oppure sul motore selezionato, quindi scegliere *Distribuisci regole*.
3. Contrassegnare con un segno di spunta le regole che si intende distribuire. Fare clic su *OK*.

4. Per avviare la regola, è necessario spostarla sotto un motore di correlazione.

NOTA: Le regole sono abilitate per la distribuzione.

---

5. Selezionare la regola posizionata sotto il motore di correlazione, quindi fare clic con il pulsante destro del mouse e scegliere *Abilita regola*.

Visualizzazioni server

Le visualizzazioni server consentono di:

- Monitorare lo stato di tutti i processi del server Sentinel nel sistema.
  - Communication Server
  - Motore di correlazione
  - DAS_Binary
  - DAS_iTRAC
  - DAS_Query
  - DAS_RT
  - Gestione delle interrogazioni
  - Verifica RuleLg
  - Sonic Lock Remover

NOTA: In Windows, Communication Server viene eseguito come servizio e pertanto non può essere monitorato nella visualizzazione server. Per monitorare Communication Server in Windows, utilizzare lo strumento di gestione dei servizi di Windows.

Il processo Sonic Lock Remover è abilitato soltanto in Windows. Se un processo non è abilitato in un determinato server, il valore nella colonna Abilitato risulterà “0” e quello nella colonna Stato sarà NOT_INITIALIZED

ALL GROUP BY SERVER HOSTNAME

	Starts	AutoRestarts	StartTime	State	UpTime	Version
Processes Health						
desk1						
Communication Server	0	0		NOT_INITIALIZED		5.1.2.0
Correlation Engine	1	0	04/17/2006 11:43:3...	Running	18h 45:53	5.1.2.0
DAS_Aggregation	1	0	04/17/2006 11:43:1...	Running	18h 46:14	5.1.2.0
DAS_Binary	1	0	04/17/2006 11:43:1...	Running	18h 46:14	5.1.2.0
DAS_Query	1	0	04/17/2006 11:43:1...	Running	18h 46:14	5.1.2.0
DAS_RT	1	0	04/17/2006 11:43:1...	Running	18h 46:14	5.1.2.0
DAS_iTRAC	1	0	04/17/2006 11:43:1...	Running	18h 46:14	5.1.2.0
Query Manager	1	0	04/17/2006 11:43:3...	Running	18h 45:54	5.1.2.0
RuleLg Checker	1	0	04/17/2006 11:43:3...	Running	18h 45:54	5.1.2.0
Sonic Lock Remover	1	0	04/17/2006 11:43:1...	Running	18h 46:15	5.1.2.0

Ready | Refresh | Options | Refreshed At: Tue Apr 18 06:29:34 EDT 2006

- Avvio, arresto o riavvio di processi: queste azioni possono essere eseguite su un processo facendo clic con il pulsante destro del mouse su di esso.

NOTA: Le operazioni accessibili con clic sul pulsante destro del mouse su Communication Server non sono abilitate poiché l'arresto di Communication Server determinerebbe la perdita di contatto con tutti i processi.

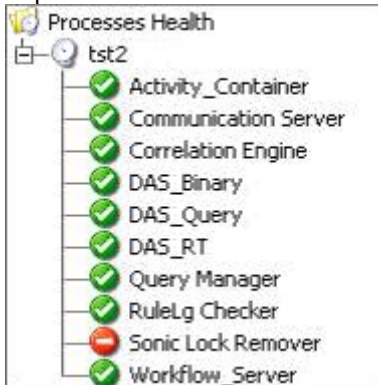
I termini avvii e riavvii automatici, nel contesto della visualizzazione server, vengono definiti nel modo seguente:

- Avvii: indica il numero di volte in cui il processo è stato avviato, per qualsiasi ragione. Indica quante volte è stato avviato il processo, per qualsiasi motivo, compresi gli avvii eseguiti dall'utente tramite interfaccia utente grafica o quelli eseguiti automaticamente.
- Riavvii automatici: indica il numero di volte in cui il processo è stato riavviato automaticamente. Questi ultimi si applicano unicamente alle operazioni automatiche e non possono quindi fare riferimento ai riavvii eseguiti dall'utente. Questo campo è utile per determinare se il processo non è riuscito (ad esempio, a causa di un errore) ed è quindi stato riavviato automaticamente dal servizio di sorveglianza di Sentinel.

Monitoraggio di un processo

Monitoraggio di un processo

1. Fare clic sulla scheda *Amministratore*.
2. Fare clic su *Visualizzazione server*.

3. Fare doppio clic su una visualizzazione. Verrà aperta una visualizzazione.
4. Espandere la visualizzazione del server. Verranno elencati tutti i processi.

Creazione di una visualizzazione server

Creazione di una visualizzazione server

1. Fare clic sulla scheda *Amministratore*.
2. Fare clic su *Visualizzazione server*.

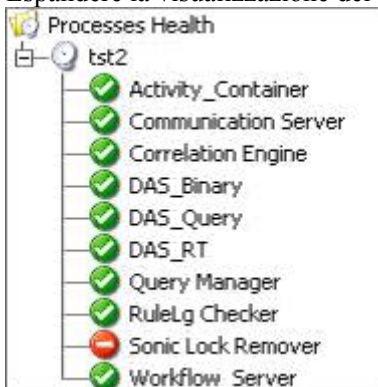
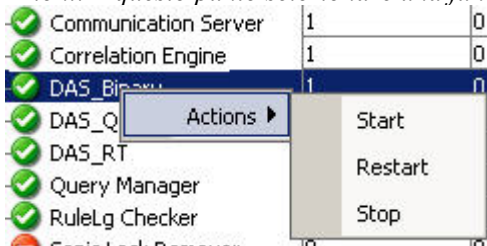
3. Per creare una nuova visualizzazione, fare clic sul pulsante *Aggiungi visualizzazione*.
   - Immettere un valore nel campo Nome opzione.
   - Per determinare i campi da visualizzare, fare clic sul pulsante *Campi*.
   - Per raggruppare titoli diversi, fare clic sul pulsante *Raggruppa per*.
   - Per ordinare in base al titolo, fare clic sul pulsante *Ordina*.
   - Per applicare un filtro, fare clic sul pulsante *Filtro*.
4. Fare clic su *OK*, quindi su *Salva*.

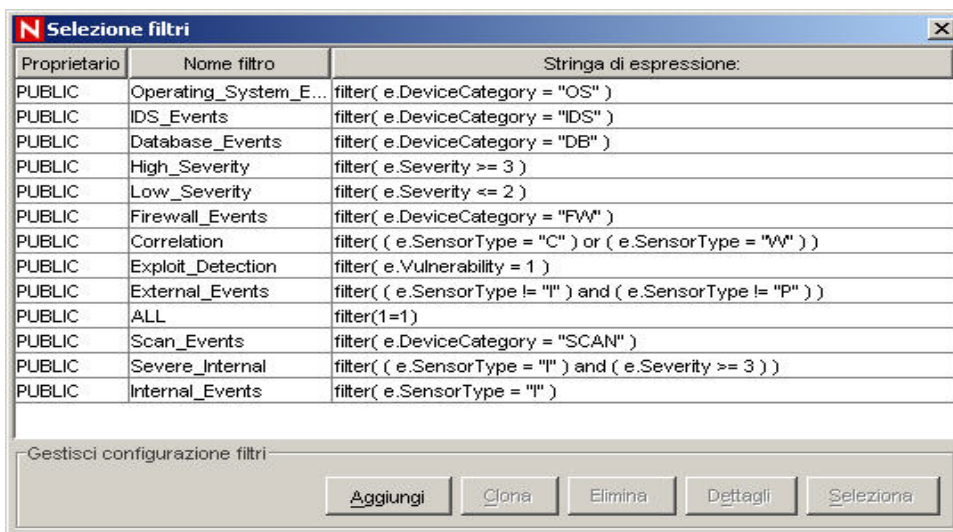
Avvio, arresto e riavvio di processi

Communication Server non può essere arrestato utilizzando questa funzione.

Avvio, arresto e riavvio di processi

1. Fare clic sulla scheda *Amministratore*.
2. Fare clic su *Visualizzazione server*.

3. Fare doppio clic su una visualizzazione. Verrà aperta una visualizzazione.
4. Espandere la visualizzazione del server. Verranno elencati tutti i processi.

5. Selezionare un processo, fare clic con il pulsante destro del mouse, *quindi scegliere Azioni. A questo punto selezionare una funzione (Avvia, Riavvia o Interrompi).*

Gestione filtri

I filtri consentono di elaborare i dati sulla base di criteri specifici sia per gli eventi in tempo reale, sia per gli utenti del sistema. I filtri consentono di gestire i dati visualizzati in Sentinel Control Center. Le finestre Evento tempo reale vengono gestite dal Motore filtri, mantenendo intatta la struttura dati di ogni filtro di sicurezza. I filtri impediscono agli utenti di visualizzare eventi non autorizzati e abbandonano gli eventi che gli utenti non intendono visualizzare. I filtri vengono creati nella scheda Amministratore di Sentinel Control Center.

NOTA: I caratteri seguenti non possono essere utilizzati nei nomi dei filtri: $ # . * & : < >.

Esistono tre tipi di filtri:

- Filtri pubblici
- Filtri privati
- Filtri globali

Filtri pubblici

I filtri pubblici sono di proprietà del sistema. I filtri pubblici possono essere utilizzati come filtri di sicurezza o filtri di visualizzazione. I filtri di sicurezza sono basati sulle autorizzazioni utente. I filtri di visualizzazione determinano gli eventi che sono illustrati nelle tabelle di eventi in tempo reale e nei grafici.

Proprietario	Nome filtro	Stringa di espressione:
PUBLIC	Operating_System_E...	filter(e.DeviceCategory = "OS")
PUBLIC	IDS_Events	filter(e.DeviceCategory = "IDS")
PUBLIC	Database_Events	filter(e.DeviceCategory = "DB")
PUBLIC	High_Severity	filter(e.Severity >= 3)
PUBLIC	Low_Severity	filter(e.Severity <= 2)
PUBLIC	Firewall_Events	filter(e.DeviceCategory = "FW")
PUBLIC	Correlation	filter((e.SensorType = "C") or (e.SensorType = "W"))
PUBLIC	Exploit_Detection	filter(e.Vulnerability = 1)
PUBLIC	External_Events	filter((e.SensorType != "I") and (e.SensorType != "P"))
PUBLIC	ALL	filter(1=1)
PUBLIC	Scan_Events	filter(e.DeviceCategory = "SCAN")
PUBLIC	Severe_Internal	filter((e.SensorType = "I") and (e.Severity >= 3))
PUBLIC	Internal_Events	filter(e.SensorType = "I")

Filtri privati

I filtri privati sono di proprietà dell'utente. Si tratta di filtri di visualizzazione che possono essere condivisi se si dispone dell’autorizzazione a visualizzarli.

Filtri globali

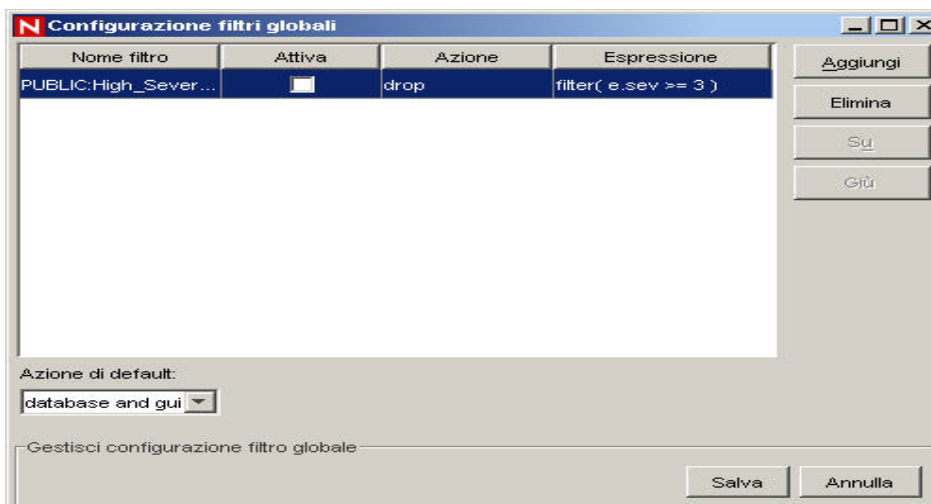
I filtri globali vengono classificati come filtri pubblici. L'elaborazione avviene in Gestione servizi di raccolta in modo sequenziale per ogni evento, fino all'individuazione di una corrispondenza. A questo punto la valutazione dei filtri globali si interrompe per quell'evento e viene eseguita l'operazione di filtro globale corrispondente. L'ordine di valutazione dei filtri globali è dall'alto verso il basso, come illustrato nella Console. Possono inoltre essere abilitati o disabilitati, in base alle esigenze.

Funzioni dei filtri globali:

- Consentono di abilitare azioni globali negli eventi. Ad esempio, abbandono di eventi, indirizzamento di eventi solo verso il database o indirizzamento di eventi verso il database e Sentinel Control Center.
- Vengono elaborati tramite la Gestione servizi di raccolta della procedura guidata.
- Vengono configurati nella scheda Amministratore, nell'opzione Configurazione filtri globali, dove possono essere abilitati o disabilitati.
- Consentono di abbandonare eventi.
- Possono indirizzare gli eventi solo verso il database.
- Possono indirizzare gli eventi verso il database e verso Sentinel Control Center.

Nella finestra Configurazione globale è possibile eseguire le operazioni seguenti:

- Creazione di filtri globali
- Riorganizzazione di filtri globali

- Eliminazione di filtri globali

Creazione di filtri globali

Per creare filtri globali

1. Fare clic sulla scheda *Amministratore*.
2. Fare clic su *Amministratore, quindi su Configurazione filtri globali* oppure selezionare *Configurazione filtri globali nell'albero* di navigazione.
3. Nella finestra Configurazione filtri globali fare clic su *Modifica*, quindi su *Aggiungi*.
4. Fare clic sulla colonna Nome *filtro nella* nuova riga vuota.
5. Selezionare un filtro, quindi fare clic su Seleziona o *Aggiungi* (se si intende creare un filtro).
6. Nella colonna Attiva selezionare *la casella corrispondente*.
7. Nella colonna Azione selezionare l'azione che verrà eseguita sugli eventi che passano questo filtro globale. Se l'evento non corrisponde a nessuno dei filtri globali attivi, l'azione di default determinerà le modalità di gestione dell'evento.

   Nella casella Azione di default sono disponibili le opzioni seguenti:

   - abbandonare: gli eventi non verranno indirizzati verso Sentinel Control Center o il database del server Sentinel.
   - database: gli eventi verranno indirizzati direttamente verso il database, ignorando Sentinel Control Center.
   - database e interfaccia grafica utente: gli eventi verranno indirizzati verso Sentinel Control Center e il database del server Sentinel.
8. Procedere finché non sono stati aggiunti tutti i filtri.
9. Fare clic su Salva.

Riorganizzazione dei filtri globali

Per riorganizzare i filtri globali

1. Nella finestra Configurazione filtri globali fare clic su *Modifica*.
2. Selezionare un filtro, quindi fare clic sul *pulsate* Su o Giù per modificarne la posizione nell'elenco.

3. Fare clic su *Salva*.

Eliminazione dei filtri globali

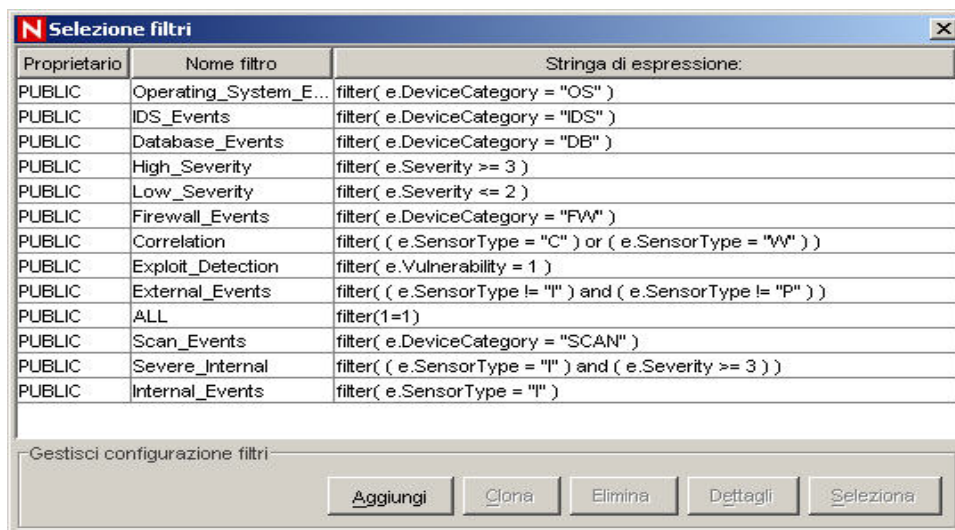
NOTA: L'eliminazione dei filtri globali non è accompagnata da alcun messaggio di conferma.

Per eliminare i filtri globali

1. Nella finestra *Configurazione filtri globali* fare clic su *Modifica*.
2. Selezionare un filtro dall'elenco e fare clic su Elimina.
3. Fare clic su *Salva*.

Configurazione dei filtri pubblici e privati

La configurazione dei filtri pubblici e privati consente di eseguire le operazioni seguenti:

- Aggiunta di un filtro
- Clonazione di un filtro
- Modifica di un filtro
- Visualizzazione dei dettagli di un filtro
- Eliminazione di un filtro

Aggiunta di un filtro

Per aggiungere un filtro pubblico e privato

1. Fare clic sulla scheda *Amministratore*.
2. Fare clic su Amministratore*, quindi su Gestione filtri* oppure *selezionare Gestione filtri nella cartella Configurazione* filtri della barra di spostamento.
3. Fare clic su *Aggiungi*.
4. Selezionare un ID proprietario pubblico o privato (di proprietà dell'utente).

5. Immettere un nome per il filtro.
6. L'editor di tabelle verrà proposto di default per la modifica dei contenuti.

NOTA: In alternativa è possibile fare clic su Usa editor formato libero, per visualizzare un editor di formato libero. L'editor di formato libero consente di creare espressioni complesse non disponibili nell'editor di tabelle. Tuttavia, una volta modificata l'espressione con l'editor di formato libero, non sarà più possibile utilizzare l'editor di tabelle nell'espressione.

7. Selezionare i criteri per le colonne seguenti:
   - Proprietà
   - Operatore
   - Colonne Valore

   Le scelte effettuate verranno visualizzate nella casella Espressione.
8. Selezionare una delle opzioni seguenti nella casella Corrispondenza se:
   - Vengono soddisfatte tutte le condizioni (and)
   - Vengono soddisfatte una o più condizioni (or)
9. Per creare un'ulteriore espressione, fare clic sul pulsante *Crea una nuova espressione di filtro* (+). Verrà aggiunta una nuova riga alla tabella dell'espressione.

10. Per rimuovere un'espressione di filtro, selezionarla dalla tabella e fare clic sul pulsante Rimuovi l'espressione selezionata (-).
11. Fare clic su Salva.

Clonazione dei filtri pubblici e privati

La clonazione è un metodo efficace che consente di duplicare un filtro e garantire la coerenza dei criteri all'interno di un gruppo di filtri o di utenti.

Per clonare un filtro pubblico e privato

1. Aprire la finestra Gestione filtri.
2. Fare clic su *Clona*.
3. Immettere un nome per il nuovo filtro.
4. Modificare eventuali criteri del filtro originale.
5. Fare clic su *Salva*.

Modifica dei filtri pubblici e privati

Per modificare un filtro pubblico e privato

1. Aprire la finestra Gestione filtri.
2. Selezionare un filtro e fare clic su *Dettagli*.
3. Modificare eventuali criteri, in base alle esigenze. L'ID proprietario e il *Nome filtro* non potranno essere modificati.
4. Fare clic su *Salva*.

Visualizzazione dei dettagli dei filtri pubblici e privati

Per visualizzare i dettagli di un filtro pubblico e privato

1. Aprire la finestra Gestione filtri.
2. Selezionare un filtro e fare clic su *Dettagli*.

Eliminazione dei filtri pubblici e privati

Per eliminare un filtro pubblico e privato

1. Aprire la *finestra Gestione filtri*.
2. Selezionare un filtro e fare clic su *Elimina*.
3. Verrà visualizzata una finestra di conferma.

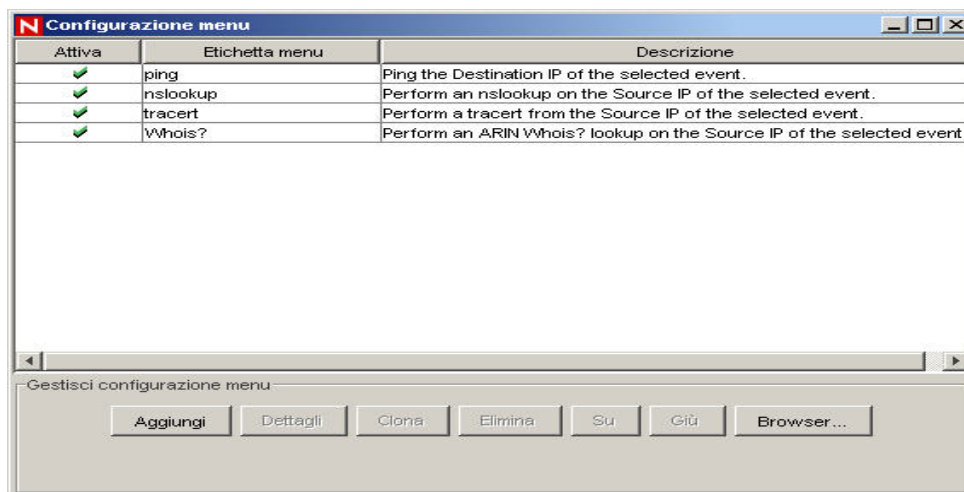
Configurazione della finestra Configurazione menu

Per utilizzare questa funzione, è necessario disporre dell'autorizzazione utente Configurazione menu.

Utilizzare la finestra Configurazione menu per creare le voci di menu che vengono visualizzate nel menu Evento. Questo menu viene richiamato facendo clic con il pulsante destro del mouse su uno o più eventi selezionati e viene visualizzato in tutte le tabelle relative agli eventi (ad esempio, la finestra Tempo reale evento, Istantanea, Casi, Eventi e così via). In Sentinel sono disponibili le seguenti voci della finestra Configurazione menu che possono essere clonate, attivate o disattivate:

- ping: esegue il ping dell'indirizzo IP di destinazione dell'evento selezionato.
- nslookup: esegue il comando di ricerca nslookup nell'indirizzo IP origine dell'evento selezionato.
- traceroute (tracert in MS SQL): esegue il comando di ricerca traceroute dall'indirizzo IP origine dell'evento selezionato al server Sentinel.
- Whois?: esegue il comando di ricerca ARIN Whois? nell'indirizzo IP origine dell'evento selezionato.

La finestra Configurazione menu consente di eseguire le operazioni seguenti:

- Aggiunta di un'opzione alla finestra Configurazione menu
- Clonazione di un'opzione della finestra Configurazione menu
- Modifica di un'opzione della finestra Configurazione menu
- Visualizzazione dei parametri di un'opzione della finestra Configurazione menu
- Attivazione o disattivazione di un'opzione della finestra Configurazione menu
- Riorganizzazione delle opzioni del menu Evento
- Eliminazione di un'opzione dalla finestra Configurazione menu
- Aggiunta di un'impostazioni browser nella finestra Configurazione menu

Aggiunta di un’opzione alla finestra Configurazione menu

NOTA: Se è stato rinominato un tag (ad esempio, se il tag CustomerVar24 è stato rinominato in PolicyName), è necessario utilizzare il nuovo nome durante l'impostazione dei parametri.

Per aggiungere un'opzione alla finestra Configurazione menu

1. Fare clic sulla scheda *Amministratore*.
2. Nella barra di spostamento fare clic su *Amministratore* > *Configurazione menu*.
3. Nella finestra di dialogo Configurazione menu specificare i dati necessari nei campi seguenti:
   - Nome
   - Descrizione
   - Azione: consente di eseguire un comando o di avviare un browser.
   - Usa browser: questa opzione può essere selezionata solo se si indica Esegui comando nel campo Azione e se il browser in uso è impostato su Usa browser esterno (per ulteriori informazioni sulla modifica delle impostazioni del browser,

vedere la sezione Modifica delle impostazioni browser della finestra Configurazione menu). Se si seleziona questa opzione, l'output del comando verrà visualizzato utilizzando le impostazioni del browser della finestra Configurazione menu per Sentinel Control Center.

- Tipo file: il tipo di file per l'output del comando può essere impostato in questo campo solo se è stata selezionata l'opzione Esegui comando nel campo Azione, il browser in uso è impostato su Usa browser esterno e l'opzione Usa browser è stata selezionata.
- Riga di comando/URL

NOTA: Per UNIX, lo script e/o l'applicazione oppure il collegamento simbolico allo script e/o all'applicazione deve essere ubicato nella directory $ESEC_HOME\sentinel \exec. Per ogni script, applicazione o collegamento simbolico immettere solo il comando. Qualsiasi percorso immesso verrà ignorato.

NOTA: Per Windows (correlazione), è necessari posizionare lo script e/o l'applicazione in una delle directory elencate nelle variabili d'ambiente di Windows. Qualsiasi percorso immesso verrà ignorato.

NOTA: Per Windows (senza correlazione), l'immissione di un percorso è facoltativa. Se si immette un comando senza specificare alcun percorso, il sistema rileverà quello di default (%ESEC_HOME%\sentinel\bin), nonché tutti quelli specificati nelle variabili d'ambiente.

- Parametri: devono essere racchiusi dal segno di percentuale, ad esempio %EventName%

NOTA: Per un elenco dei tag disponibili che è possibile utilizzare durante la definizione dei parametri, fare clic su ? nella finestra di dialogo Configurazione menu oppure vedere il capitolo relativo al tag META nella *Guida di riferimento dell'utente di Sentinel*.

---

4. Fare clic su *OK*. La nuova opzione verrà aggiunta all'elenco di voci di menu nella finestra Configurazione menu.

NOTA: Per visualizzare un esempio, selezionare una voce di menu di default e scegliere Dettagli. Nella figura seguente è illustrata una configurazione per il comando di ricerca nslookup:

Clonazione di un’opzione della finestra Configurazione menu

Per clonare un'opzione della finestra Configurazione menu

1. Aprire la finestra Configurazione menu.
2. Selezionare una voce di menu dalla tabella e fare clic su *Clona*.
3. Nella finestra di dialogo Configurazione menu modificare i dati seguenti:
   - Nome
   - Descrizione
   - Azione
   - Utilizzo di un browser o meno. Per ulteriori informazioni, vedere la sezione Aggiunta di una impostazioni browser nella finestra Configurazione menu.
   - Riga di comando/URL
   - Parametri
   - Selezionare un'azione:
     - Esegui comando
     - Avvia browser Web

   NOTA: Per un elenco dei tag disponibili che è possibile utilizzare durante la definizione dei parametri, fare clic su ? nella finestra di dialogo Configurazione menu oppure vedere il capitolo relativo al tag META nella Guida di riferimento dell'utente di Sentinel.

4. Fare clic su *OK*. La nuova opzione verrà aggiunta all'elenco di voci di menu nella finestra Configurazione menu.

Modifica di un’opzione della finestra Configurazione menu

Per modificare un'opzione della finestra Configurazione menu

1. Aprire la finestra Configurazione menu.
2. Fare doppio clic su un'opzione di menu.
3. Digitare le modifiche necessarie, quindi fare clic su *OK*.

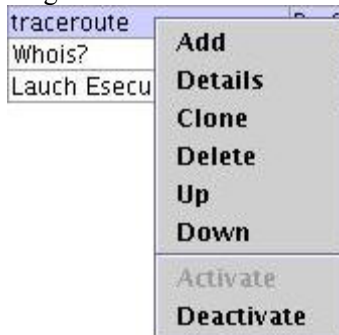
Visualizzazione dei parametri di un'opzione della finestra Configurazione menu

Per visualizzare i parametri di un'opzione della finestra Configurazione menu

1. Aprire la finestra Configurazione menu.
2. Evidenziare una voce di menu e scegliere *Dettagli*.

Attivazione o disattivazione di un’opzione della finestra Configurazione menu

Per attivare o disattivare un'opzione della finestra Configurazione menu

1. Aprire la finestra Configurazione menu.
2. Selezionare un'opzione di menu, fare clic con il pulsante destro del mouse, quindi scegliere *Attiva* o *Disattiva*.

Riorganizzazione delle opzioni del menu Evento

Per spostare un'opzione del menu Evento verso l'alto il basso

1. Aprire la finestra Configurazione menu.
2. Selezionare un'opzione di menu, quindi scegliere Su o Giù.

Eliminazione di un’opzione della finestra Configurazione menu

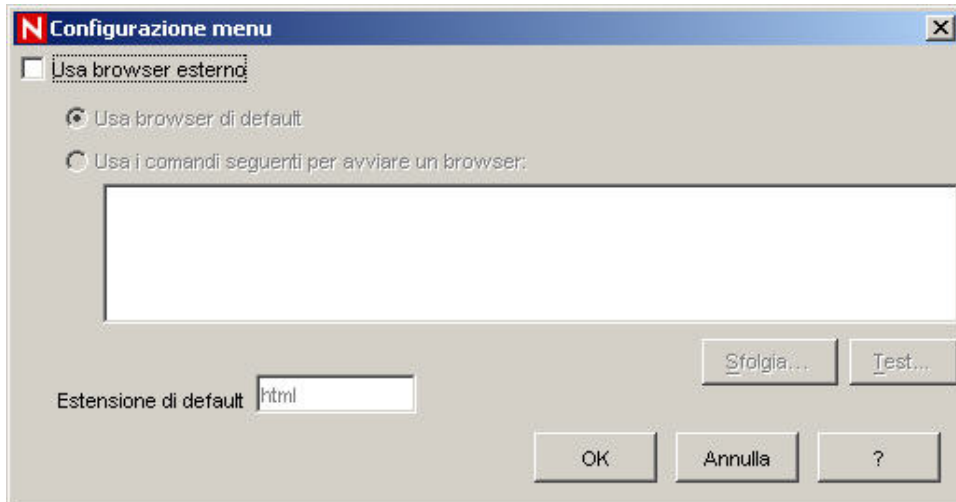
Per eliminare un'opzione della finestra Configurazione menu

1. Aprire la finestra Configurazione menu.
2. Selezionare un'opzione di menu e fare clic su Elimina.
   - Per eliminare l'opzione di menu, fare clic su Sì.
   - Per mantenere l'opzione di menu, fare clic su No.

Modifica delle impostazioni browser della finestra Configurazione menu

Questa opzione consente di inviare l'output delle opzioni della finestra Configurazione menu a un browser esterno. Il browser esterno può essere una qualsiasi applicazione. Non è necessario che si tratti di browser Internet. Modificando l'estensione del file è possibile avviare qualsiasi applicazione sia associata all'estensione. Ad esempio, l'estensione TXT è di norma associata all'applicazione Blocco note. Tuttavia, si può scegliere di aprire il file TXT con un programma specifico, quale WordPad o un altro editor di testo.

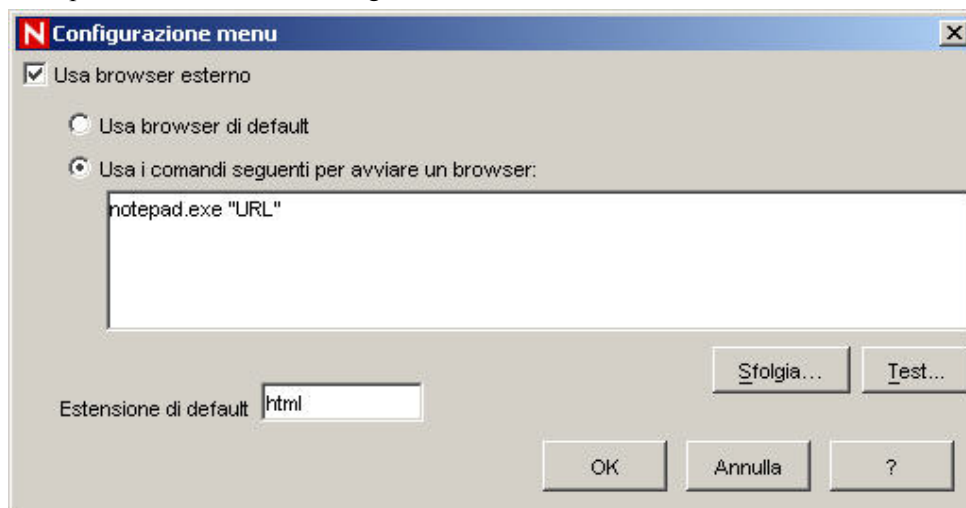
Per modificare le impostazioni del browser della finestra Configurazione menu

1. Aprire la finestra Configurazione menu.
2. Fare clic su *Browser*.

Se, durante l'impostazione dell'opzione della finestra Configurazione menu, l'opzione Usa browser viene selezionata insieme alla funzione browser di default (come illustrato nella figura), l'opzione della finestra Configurazione menu si comporterà come se la casella Usa browser non fosse stata selezionata.

Se si seleziona la casella Usa browser esterno, sarà possibile eseguire una delle operazioni seguenti:

- Usa browser di default: consente di utilizzare il browser (applicazione) di default associato all'estensione del file impostata nel relativo campo.
- Usa i comandi seguenti per avviare un browser: consente di indicare un'applicazione specifica da avviare. Se si utilizza un browser diverso da quello di default, la riga di comando deve essere seguita da un parametro %URL%. Ad esempio:

  ```
  C:\Programmi\Internet Explorer\IEXPLORE.EXE %URL%
  ```

Nella figura seguente è stata specificata l'applicazione Blocco note per l'output dell'opzione della finestra Configurazione menu.

3. Fare clic su *OK* al termine della configurazione.

Statistiche DAS

Questa funzione consente di eseguire il monitoraggio interno del sistema. La funzione non è destinata a utenti con competenze di livello medio. Statistiche DAS consente di monitorare quanto segue:

- DAS_Binary
- DAS_Query
- DAS_rt

Le statistiche sono suddivise in:

- Servizio: nome del servizio. Ad esempio, DAS_Query
- Ora: tempo trascorso dall'ultimo aggiornamento
- Num: numero di richieste elaborate per la voce
- Attesa (sec.): tempo medio di attesa (espresso in secondi) prima che l'elaborazione di una richiesta venga avviata
- Esecuzione (sec.): tempo medio (espresso in secondi) per l'elaborazione di una richiesta
- #In attesa: dimensione media della coda di attesa
- #Esecuzione: dimensione media della coda di esecuzione

Queste informazioni sono suddivise in 3 sezioni:

- Richieste
- Servizi
- Pool di thread

Nella sezione Richieste sono indicate tutte le richieste per canale (ad esempio, services.CorrelationService). Nella sezione Servizi sono indicate tutte le richieste per servizio. In alcuni casi viene creata un'ulteriore suddivisione, aggiungendo la <categoria> sotto il nome. Ad esempio Services.CorrelationService oppure Services.RemoteObjectService.EMap.get MapPK.

Nella sezione Servizi, inoltre, tutte le chiamate al metodo remoto dai servizi definiti dall'utente (i servizi XML) sono indicate sotto services.RemoteObjectService. Viene quindi indicato il nome del servizio (EMap nell'esempio sopra citato), nonché il nome del metodo (getMapPK nell'esempio sopra citato), se richiesto.

Quando un server riceve una richiesta, come una query dal server DAS, viene creato e pianificato un task. Tale task viene quindi assegnato a un pool di thread. Possono esistere più pool di thread, ognuno dei quali può essere utilizzato per più servizi. Per questo motivo può accadere che una richiesta debba essere messa in attesa di un thread disponibile, sebbene il servizio non sia molto utilizzato. Verificare le informazioni relative ai pool di thread, qualora nelle statistiche venga indicato che il tempo di attesa è elevato e che il numero di richieste per quel servizio è basso.

Il numero accanto alla voce indica il totale dei figli della richiesta. Ad esempio, il numero 15 indica che sono presenti 15 richieste per tutte le chiamate al metodo richieste. Ne consegue che requests.configurations 1 indica che una delle 15 richieste è per le configurazioni, mentre requests.esecurity.correlation.config 2 indica che due delle 15 richieste sono per esecurity.correlation.config e così via.

Servizio	Ora	Nome	Num	Attesa (sec.)	Esecuzione (se...	#In attesa	#Esecuzione
DAS_Query-289...	19.00.00						
		ThreadPools	348	0,001	0,002	0,0	0,0
		ThreadPools.Def...	59	0,005	0,009	0,0	0,0
		ThreadPools.Def...	15	0,001	0,015	0,0	0,0
		ThreadPools.Def...	0			0,0	0,0
		ThreadPools.Def...	0			0,0	0,0
		ThreadPools.Def...	0			0,0	0,0
		ThreadPools.Def...	29	0,010	0,011	0,0	0,0
		ThreadPools.Def...	0			0,0	0,0
		ThreadPools.Def...	15	0,000	0,000	0,0	0,0
		ThreadPools.Def...	0			0,0	0,0
		ThreadPools.Tim...	289	0,000	0,001	0,0	0,0
		ThreadPools.Tim...	1	0,000	0,000	0,0	0,0
		ThreadPools.Tim...	15	0,000	0,005	0,0	0,0
		ThreadPools.Tim...	0			0,0	0,0
		ThreadPools.Tim...	1	0,078	0,062	0,0	0,0
		ThreadPools.Tim...	180	0,000	0,000	0,0	0,0
		ThreadPools.Tim...	90	0,000	0,000	0,0	0,0
		ThreadPools.Tim...	2	0,000	0,008	0,0	0,0
		ThreadPools.Tim...	0			0,0	0,0
		ThreadPools.Tim...	0			0,0	0,0
		requests	119	0,026	0,005	0,0	0,0
		requests.LOGIN...	0			0,0	0,0
		requests.config...	0			0,0	0,0

Questa informazione può essere utile, in quanto fornisce un'idea di ciò che sta accadendo. Il numero di richieste, in modo particolare, consente di vedere dove si concentrano le richieste. Nella colonna #In attesa è possibile rilevare se il server è occupato. Il numero non dovrebbe essere elevato. Se così non fosse, le nuove richieste (anche per task semplici) dovranno attendere che vengano eseguite prima quelle potenzialmente lente. Non è una situazione ottimale. Il tempo medio di esecuzione è molto importante, in quanto indica quali richieste stanno occupando il server.

Informazioni su file di evento

Nel riquadro superiore vengono visualizzate le informazioni di stato per ogni file di evento, Lo stato fa riferimento ai file di evento al momento dell'apertura della finestra. Nel riquadro non verrà indicato lo stato di eventuali file di evento precedenti. Nel riquadro vengono inoltre visualizzati l'ID del file (ovvero, arch_id nella tabella eventi), il nome del file e le relative statistiche (ad esempio, se il file è completo, l'ora di inizio e di fine della scrittura del file, il numero minimo e massimo di eventi contenuti nel file e così via).

Quando si seleziona un file di evento nel riquadro superiore, il relativo stato riepilogativo viene visualizzato nel riquadro inferiore. Questo riquadro contiene le informazioni seguenti: nome del riepilogo, ora di inizio e di fine dell'elaborazione del file, numero di eventi elaborati ed eventuali messaggi di errore.

Configurazioni utente

Per utilizzare questa funzione, è necessario disporre dell'autorizzazione utente Configurazione utente, che consente di lavorare nella finestra omonima.

La finestra Configurazione utente consente di eseguire le operazioni seguenti:

- Configurazione di un conto utente
- Modifica di un conto utente
- Visualizzazione dei dettagli di un conto utente
- Clonazione di un conto utente
- Eliminazione di un conto utente
- Termine di una sessione attiva
- Aggiunta di un ruolo iTRAC
- Eliminazione di un ruolo iTRAC
- Dettagli di un ruolo iTRAC

Il programma di installazione creerà gli utenti di default seguenti sul server Sentinel:

Autenticazione Oracle e MS SQL:

- esecdba: proprietario dello schema (configurabile in fase di installazione).
- esecadm: utente amministratore di Sentinel (configurabile in fase di installazione).

NOTA: Per UNIX, il programma di installazione creerà anche l'utente del sistema operativo con gli stessi nome utente e password.

- esecrpt: utente autore rapporto, password dell'utente admin.
- ESEC_CORR: utenti del motore di correlazione, utilizzati per creare casi.
- esecapp: nome utente dell'applicazione Sentinel per la connessione al database.

Autenticazione Windows:

- Amministratore DB Sentinel: proprietario dello schema (configurabile in fase di installazione).
- Amministratore Sentinel: utente amministratore di Sentinel (configurabile in fase di installazione).

- Utente rapporto Sentinel: utente autore rapporto, password dell'utente admin.
- Utente DB dell'applicazione Sentinel: nome utente dell'applicazione Sentinel per la connessione al database.

Apertura della finestra Gestione utenti

Per aprire la finestra Gestione utenti

1. Fare clic sulla scheda *Amministratore*.
2. Fare clic su Amministratore, quindi su *Configurazione utente*.

Configurazione dei conti utente

NOTA: Per soddisfare le rigorose configurazioni di sicurezza necessarie per la certificazione dei criteri comuni, Sentinel richiede una password con le caratteristiche seguenti:

1. Scegliere password costituite da un minimo di 8 caratteri, di cui almeno uno MAIUSCOLO, uno minuscolo, uno speciale (!@#$%^&*()_+) e uno numerico (0-9).

2. Non è possibile includere nella password l'indirizzo di e-mail o una parte qualsiasi del nome completo.

3. La password non deve essere una parola “comune”, ovvero una parola inclusa nel dizionario o di uso gergale.

4. È necessario che nella password non siano incluse parole di alcuna lingua poiché esistono numerosi programmi per la violazione delle password in grado di elaborare milioni di possibili combinazioni di parole in pochi secondi.

5. È consigliabile scegliere una password facile da ricordare e allo stesso tempo complessa. Ad esempio, Mfhq5!ao (Mio Figlio Ha Quasi 5 Anni Ormai) oppure VaNdq#3a (Vivo a Napoli Da Quasi 3 anni).

Per utilizzare questa funzione, è necessario disporre dell'autorizzazione utente di creazione di un conto utente. Le autorizzazioni utente sono abbastanza dettagliate. Per ulteriori informazioni, vedere la relativa sezione nella Guida di riferimento dell'utente di Sentinel.

NOTA: È necessario che la password dell'utente esecrpt venga cambiata direttamente nel database. A tale scopo è possibile utilizzare Enterprise Manager.

Per creare un conto utente

1. Aprire la finestra Gestione utenti.
2. Fare clic sul *pulsante Aggiungi un nuovo utente*.

In alternativa, selezionare un utente, fare clic con il pulsante destro del mouse e scegliere *Aggiungi utente*.

3. In Autorizzazione immettere i dati seguenti:
   - Nome utente
   - Password
   - Conferma password
   - Filtro di sicurezza: per selezionare un filtro, fare clic sulla freccia giù. Verrà visualizzata la finestra Selezione filtri. Selezionare un filtro oppure fare clic sul pulsante Aggiungi, per creare un filtro per questo conto utente.

NOTA: Una volta assegnato a un utente, il filtro di sicurezza non può più essere eliminato.

   - Fare clic su *Seleziona*.

NOTA: La procedura consigliata prevede l'utilizzo di password composte da almeno 8 caratteri alfanumerici.

In Dettagli immettere i dati seguenti (facoltativo):
   - Nome
   - Cognome
   - Reparto
   - Telefono
   - E-mail
4. Fare clic sulla scheda *Autorizzazioni* e assegnare le autorizzazioni per l'utente.
5. Fare clic sulla scheda *Ruoli* e selezionare il ruolo per l'utente.
6. Fare clic su *OK*.

NOTA: In Oracle non è consentito creare utenti il cui nome corrisponda a una delle Parole riservate di Oracle. Inoltre, questi nomi non sono consentiti nemmeno in Sentinel.

Modifica dei conti utente

Per utilizzare questa funzione, è necessario disporre dell'autorizzazione utente di modifica del conto utente esistente.

NOTA: È necessario che la password dell'utente esecrpt venga cambiata direttamente nel database. A tale scopo è possibile utilizzare Enterprise Manager.

Per modificare un conto utente

1. Aprire la finestra Gestione utenti.
2. Fare doppio clic su un conto utente oppure fare clic con il pulsante destro del mouse e scegliere *Dettagli utente*.
3. Modificare il conto.
4. Fare clic su OK.

Visualizzazione dei dettagli dei conti utente

Per utilizzare questa funzione, è necessario disporre dell'autorizzazione utente per l'utilizzo e/o la visualizzazione del conto utente.

Per visualizzare i dettagli di un conto utente

1. Aprire la finestra Gestione utenti.
2. Fare doppio clic su un conto utente oppure fare clic con il pulsante destro del mouse e scegliere *Dettagli utente*.
3. Verificare i dettagli del conto utente, quindi chiudere la finestra.

Clonazione dei conti utente

Per clonare un conto utente

1. Aprire la finestra Gestione utenti.
2. Selezionare un ID conto utente, fare clic con il pulsante destro del mouse e scegliere *Clona utente*.
3. Modificare le informazioni e le autorizzazioni per l'utente.
4. Fare clic su *Salva*.

Eliminazione dei conti utente

Per utilizzare questa funzione, è necessario disporre dell'autorizzazione utente di eliminazione del conto utente.

NOTA: Una volta eliminato, un utente non può più essere ricreato. Ad esempio, se si crea l'utente Carlo e successivamente lo si elimina, non sarà più possibile ricreare un utente chiamato Carlo.

Per eliminare un conto utente

1. Aprire la finestra Gestione utenti.
2. Selezionare un ID conto utente, fare clic con il pulsante destro del mouse e scegliere *Elimina utente*.

Termine di una sessione attiva

Per terminare una sessione attiva

1. Aprire la finestra Sessioni utente attive.
2. Selezionare una sessione attiva che si intende terminare.
3. Fare clic con il pulsante destro del mouse e scegliere *Termina sessione*.
4. Verrà richiesto un messaggio di interruzione. Verrà richiesto di immettere un messaggio nel quale si indica il motivo per cui si interrompe la sessione.

Aggiunta di un ruolo iTRAC

Per aggiungere un ruolo iTRAC

1. Aprire la finestra Gestione ruoli.
2. Fare clic sul pulsante *Aggiungi un nuovo ruolo*.

In alternativa, fare clic con il pulsante destro del mouse e scegliere *Aggiungi nuovo ruolo*.

Eliminazione dei ruoli iTRAC

Per eliminare un ruolo iTRAC

1. Aprire la finestra Gestione ruoli.
2. Selezionare un ruolo, fare clic con il pulsante destro del mouse, quindi scegliere *Elimina ruolo*.

Dettagli dei ruoli iTRAC

Per visualizzare i dettagli di un ruolo iTRAC

1. Aprire la finestra Gestione ruoli.
2. Selezionare un ruolo, fare clic con il pulsante destro del mouse, quindi scegliere *Dettagli ruolo*.

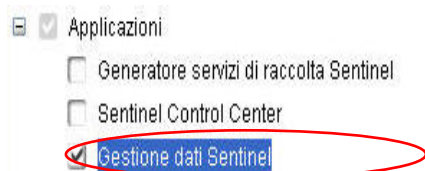
10 Gestione dati Sentinel

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Gestione dati Sentinel è uno strumento che consente gli utenti di gestire il database di Sentinel. Lo strumento consente di eseguire le attività seguenti:

- Monitorare l'utilizzo dello spazio del database
- Visualizzare e gestire le partizioni del database
- Gestire gli archivi del database
- Importare dati nel database
- Configurare la mappatura dei dati
- Configurare i nomi dei tag di evento
- Configurare le impostazioni dei rapporti di riepilogo

Installazione di Gestione dati Sentinel

È possibile installare Gestione dati Sentinel direttamente mediante la Procedura guidata InstallShield di Sentinel 5 selezionando il componente "*Gestione dati Sentinel*" nella pagina per la selezione delle caratteristiche di Sentinel 5.

Solo per Oracle, si noti che ai fini della comunicazione di Gestione dati Sentinel con i database Oracle è inoltre necessario scaricare manualmente il driver JDBC Oracle 9.2.0.4 o 9.2.0.5 e copiare il file con estensione jar scaricato nella directory $ESEC_HOME/lib nella stessa postazione in cui è stato installato Gestione dati Sentinel oppure in %ESEC_HOME%\lib in caso di installazione di Gestione dati Sentinel su Windows. È possibile scaricare il driver JDBC all'URL seguente:

NOTA: Se si utilizza un computer UNIX in cui è installato il componente DAS, il driver JDBC verrà automaticamente inserito nell'ubicazione corretta dal programma di installazione. In questo caso non è pertanto necessario il download manuale.

http://otn.oracle.com/software/tech/java/sqlj_jdbc/index.html

In genere, il nome del file con estensione jar è ojdbc14.jar.

NOTA: Alla data di pubblicazione di questa guida, l'indirizzo di tale sito Web risultava corretto.

NOTA: Gestione dati Sentinel per Oracle richiede l'installazione di Oracle Enterprise con partizionamento.

Avvio dell'interfaccia utente grafica di Gestione dati Sentinel

NOTA: Per utilizzare l'interfaccia utente grafica di Gestione dati Sentinel, è necessario che il file configuration.xml faccia riferimento a un'istanza di Communication Server connessa inoltre a DAS_Binary e DAS_Query. Si tratta in genere della situazione di default purché Communication Server e i processi DAS siano in esecuzione.

Per UNIX: avvio dell'interfaccia utente grafica di Gestione dati Sentinel

1. Eseguire il login alla postazione UNIX come membro del gruppo esec (ad esempio, esecadm).
2. Passare alla directory $ESEC_HOME/sdm
3. Immettere il comando seguente:

```
./sdm
```

Per Windows: avvio dell'interfaccia utente grafica di Gestione dati Sentinel

1. Fare clic su *Start* > *Programmi* > *Sentinel* > *Gestione dati Sentinel*

NOTA: Per eseguire Gestione dati Sentinel dalla riga di comando, vedere la sezione relativa alla riga di comando di Gestione dati Sentinel in questo documento.

Connessione al database

All'avvio di Gestione dati Sentinel, è necessario stabilire una connessione al database in uso. Nella finestra di dialogo "*Connetti al database*" immettere i valori appropriati per ogni campo.

Connessione al database

1. Avviare l'interfaccia utente grafica di Gestione dati Sentinel.
2. Selezionare il tipo di database, ovvero Oracle o MSSQL.
3. Specificare il nome dell'istanza di database, ad esempio ESEC.
4. Specificare l'host del database utilizzando il nome host o l'indirizzo IP.
5. Per quanto concerne la porta, utilizzare la porta di default 1521 per Oracle oppure la porta di default 1433 per MSSQL.
6. Utilizzare il nome utente e la password dell'amministratore del database di Sentinel, ad esempio esecdba.

NOTA: Per Windows e MS SQL, se MS SQL è stato installato in modalità mista, è possibile accedervi mediante l'autenticazione di Windows OPPURE l'autenticazione di SQL Server. Se MS SQL è stato installato solo nella modalità con l'autenticazione di Windows, sarà necessario utilizzare quest'ultima per effettuare l'accesso. Se si sceglie di utilizzare l'autenticazione di Windows, ai fini dell'autenticazione al database di MS SQL verranno utilizzate le credenziali dell'utente attualmente connesso a Windows

Per Oracle:

Per Windows:

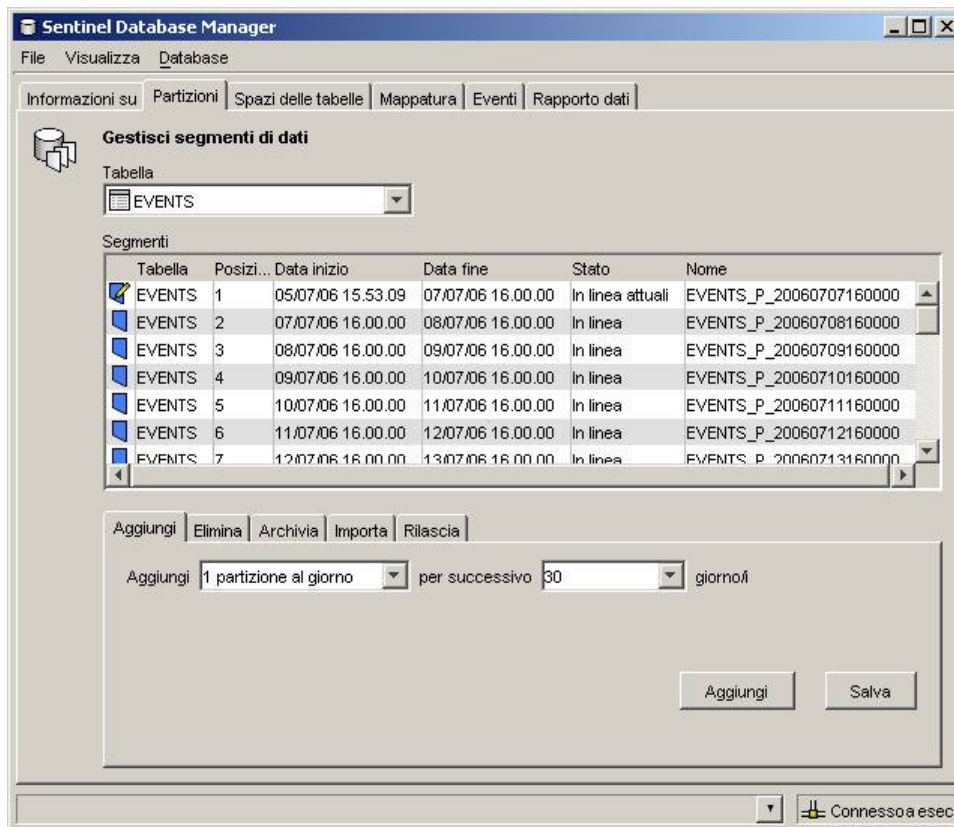
NOTA: Se si sceglie di salvare le impostazioni di connessione, queste ultime verranno memorizzate nel file sdm.connect. Al successivo avvio dell'interfaccia utente grafica, le impostazioni di connessione verranno recuperate e applicate dal file sdm.connect. È possibile utilizzare tale file quando si esegue Gestione dati Sentinel dalla riga di comando.

7. Fare clic su Connetti.

Partizioni

La scheda Partizioni di Gestione dati Sentinel consente agli utenti di visualizzare e gestire le partizioni del database.

Per visualizzare le partizioni nell'interfaccia utente grafica

1. Fare clic sulla scheda *Partizioni*.
2. Selezionare la tabella da visualizzare nell'elenco a discesa.

Nella tabella Segmenti verranno visualizzate le partizioni della tabella di database selezionata.

In ogni riga della tabella Segmenti vengono indicati la tabella del database, l'intervallo di tempo, lo stato e il nome della partizione.

Lo stato di ognuna delle partizioni indicate nella tabella Segmenti può corrispondere a uno dei valori seguenti:

In linea	i dati inclusi in una partizione in linea sono disponibili per l'accesso
In linea attuale	una partizione in linea in cui vengono attualmente inserite le righe
In linea archiviata	partizione i cui dati sono archiviati ma ancora accessibili per uno dei motivi seguenti: ▪ la partizione non è stata ancora abbandonata ▪ la partizione è stata reimportata
Non in linea	i dati in una partizione non in linea non sono disponibili per l'accesso poiché la partizione è stata abbandonata e non importata
Non in linea archiviata	partizione archiviata e abbandonata

Per gestire le partizioni

1. Fare clic sulla scheda *Partizioni*.
2. Selezionare la tabella nell'elenco a discesa.
3. Nella parte inferiore della finestra selezionare la scheda correlata all'operazione che si desidera eseguire, ovvero Aggiungi, Elimina, Archivia, Importa o Rilascia.

Per aggiungere partizioni

1. Selezionare la scheda *Aggiungi* partizioni.
2. Specificare il numero di partizioni da aggiungere e il numero di giorni durante i quali aggiungerle.
3. Premere *Aggiungi*.

Per eliminare partizioni

1. Selezionare la scheda *Elimina* partizioni.
2. Specificare il numero di giorni trascorsi i quali le partizioni devono essere eliminate.
3. Fare clic su *Elimina*.

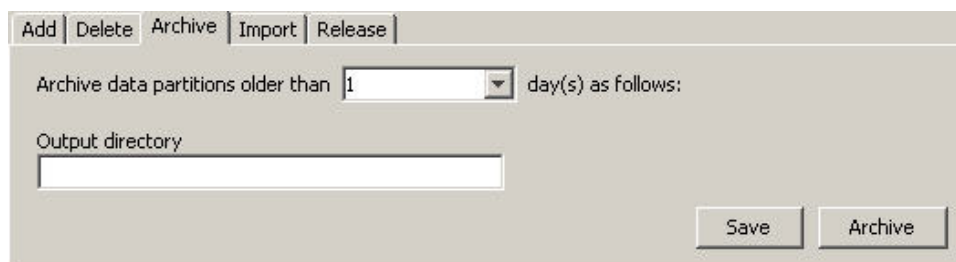
Per archiviare partizioni

NOTA: Le tabelle di aggregazione non vengono archiviate.

1. Selezionare la scheda *Archivia* partizioni.
2. Specificare il numero di giorni trascorsi i quali le partizioni devono essere archiviate e la directory in cui archiviarle.

   NOTA: Per UNIX, non è possibile archiviare le partizioni in/root.

3. Fare clic su *Archivia*.

   NOTA: Ai fini dell'archiviazione, accertarsi di specificare un percorso valido nel server del database con le autorizzazioni appropriate.

NOTA: La scheda Archivia è diversa per MSSQL e Oracle. Per Oracle è consentito specificare la dimensione massima del file di archiviazione.

Scheda Archivia relativa alle partizioni di Oracle:

Scheda Archivia relativa alle partizioni di MSSQL:

Per importare partizioni

1. Selezionare la scheda *Importa* partizioni.
2. Nella tabella Segmenti selezionare la partizione in cui importare i dati.
3. Specificare la directory di input da cui leggere i dati archiviati.
4. Fare clic su *Importa*.

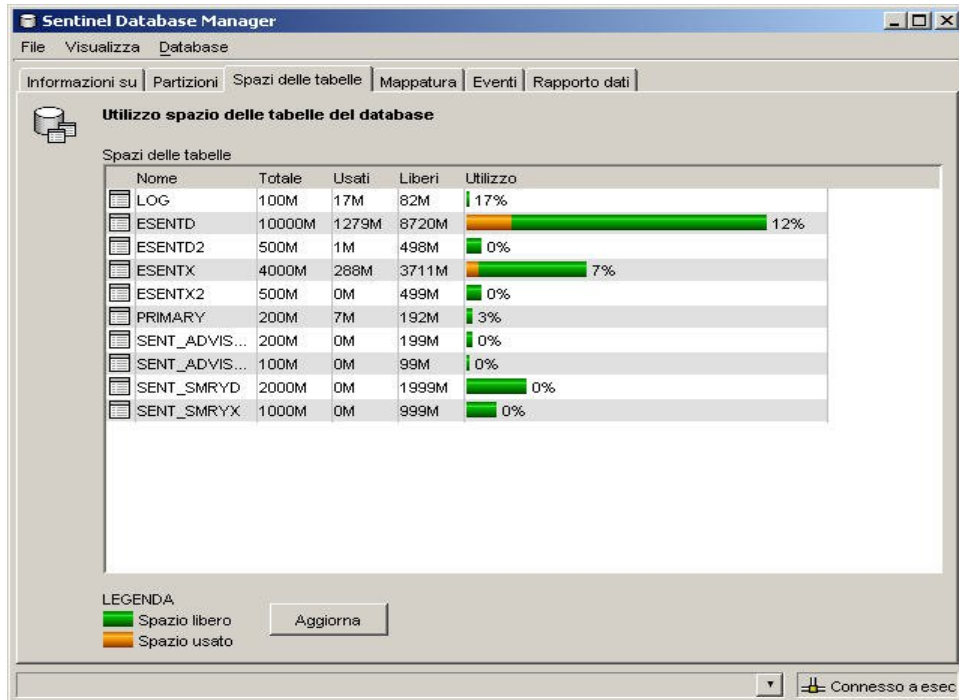
Per rilasciare partizioni importate

1. Selezionare la scheda *Rilascia* partizioni.
2. Nella tabella Segmenti selezionare la partizione da rilasciare.
3. Fare clic su *Rilascia*.

Spazi delle tabelle

La scheda Spazi delle tabelle di Gestione dati Sentinel consente agli utenti di visualizzare l'utilizzo attuale dello spazio del database.

Per visualizzare gli spazi delle tabelle nell'interfaccia utente grafica

1. Fare clic sulla scheda Spazi delle *tabelle*.

Nella tabella Utilizzo spazio delle tabelle del database vengono indicati lo spazio totale allocato per ogni spazio delle tabelle, la quantità di memoria utilizzata da ogni spazio delle tabelle e la quantità di memoria ancora disponibile (libera) per ognuno di essi. Le barre con codifica a colori agevolano la lettura dello spazio totale allocato per ogni spazio delle tabelle e la relativa percentuale.

NOTA: Gli spazi delle tabelle non sono disponibili in MS SQL, in cui vengono utilizzati i filegroup.

Scheda Mappatura

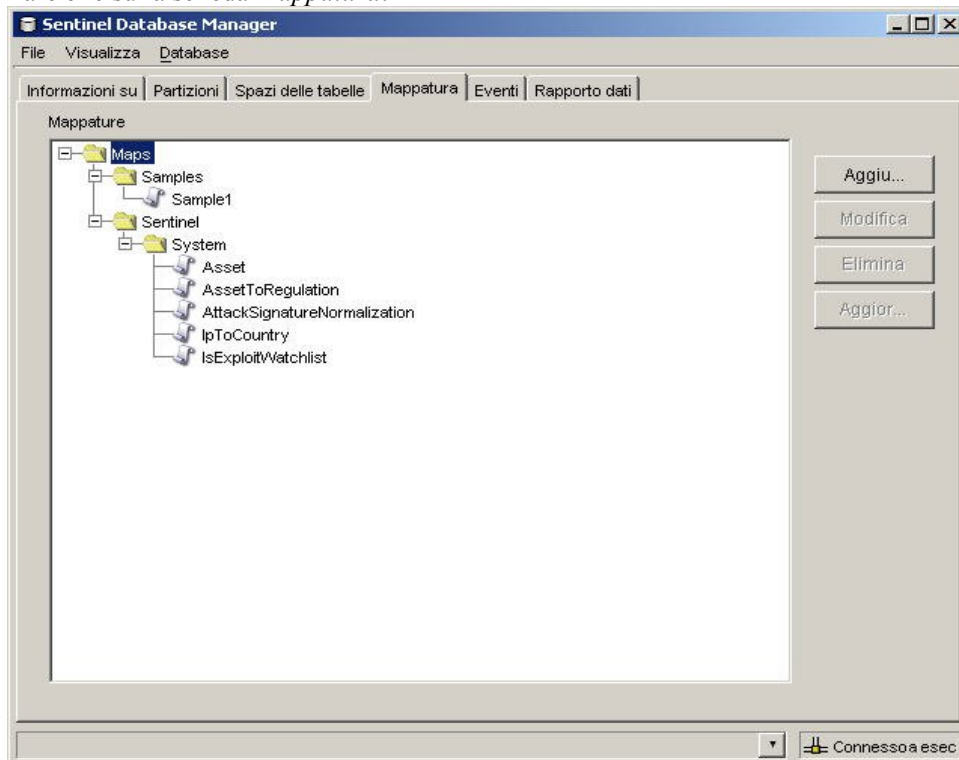
NOTA: Per utilizzare la scheda Mappatura, è necessario che il file configuration.xml faccia riferimento a un'istanza di Communication Server connessa inoltre a DAS_Binary e DAS_Query. Si tratta in genere della situazione di default purché Communication Server e i processi DAS siano in esecuzione.

La scheda Mappatura consente di:

- Aggiungere nuove definizioni di mappatura
- Modificare le definizioni di mappatura
- Eliminare le definizioni di mappatura
- Aggiornare i dati di mappatura

La mappatura funziona in combinazione con l'opzione di origine dati "*Riferimento da mappatura*" nella scheda Eventi. È possibile eseguire la mappatura mediante una stringa o un intervallo numerico.

Per visualizzare le mappature nell'interfaccia utente grafica

1. Fare clic sulla scheda *Mappatura*.

Nell'interfaccia utente grafica della scheda Mappatura principale verrà visualizzato un elenco di tutte le mappature definite nel sistema.

NOTA: Non è possibile modificare o eliminare le mappature incluse nella cartella System.

Aggiunta di definizioni di mappatura

Per aggiungere una definizione di mappatura:

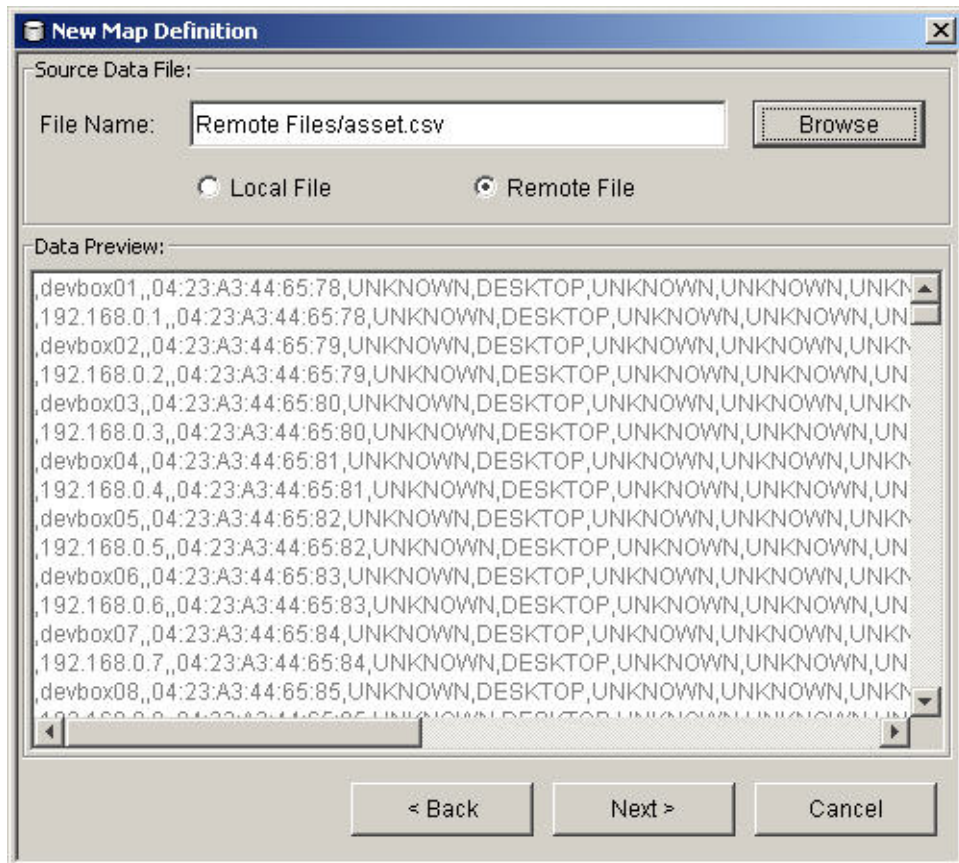
1. Fare clic sulla scheda *Mappatura*.
2. Fare clic su *Aggiungi*.
3. Se si crea una nuova cartella di mappatura, fare clic sul pulsante *Nuovo*. Immettere il nome della cartella.

   NOTA: Se si tratta della prima definizione di mappatura, è consigliabile creare una nuova cartella. Se la definizione di mappatura viene inserita nella cartella System non sarà possibile modificarla o eliminarla.

4. Verificare che la cartella in cui si desidera inserire la definizione di mappatura sia selezionata, ovvero che la cartella sia indicata come aperta.
5. Immettere il nome della mappatura.
6. Fare clic su *Avanti*.

   NOTA: La casella del campo Tipo mappatura è disabilitata.

7. Selezionare File locale o File remoto.

- File locale: consente di cercare il file nel file system locale, ovvero nel computer in cui è stato avviato Gestione dati Sentinel.
- File remoto: consente di scegliere tra i file dei dati di origine della mappatura esistente sul server in cui è in esecuzione DAS. Se Advisor è installato e i dati relativi alla vulnerabilità sono stati caricati, è possibile che sul server esistano già i file attackNormalization.csv e exploitDetection.csv. File remoto fa riferimento a %ESEC_HOME%\sentinel\bin\map_data in Windows o a $ESEC_HOME/sentinel/bin/map_data in UNIX.

Selezionare il file di definizione della mappatura. Fare clic su *Avanti*.

NOTA: I file di mappatura contenenti più di 500 righe non vengono visualizzati completamente in Gestione dati Sentinel.

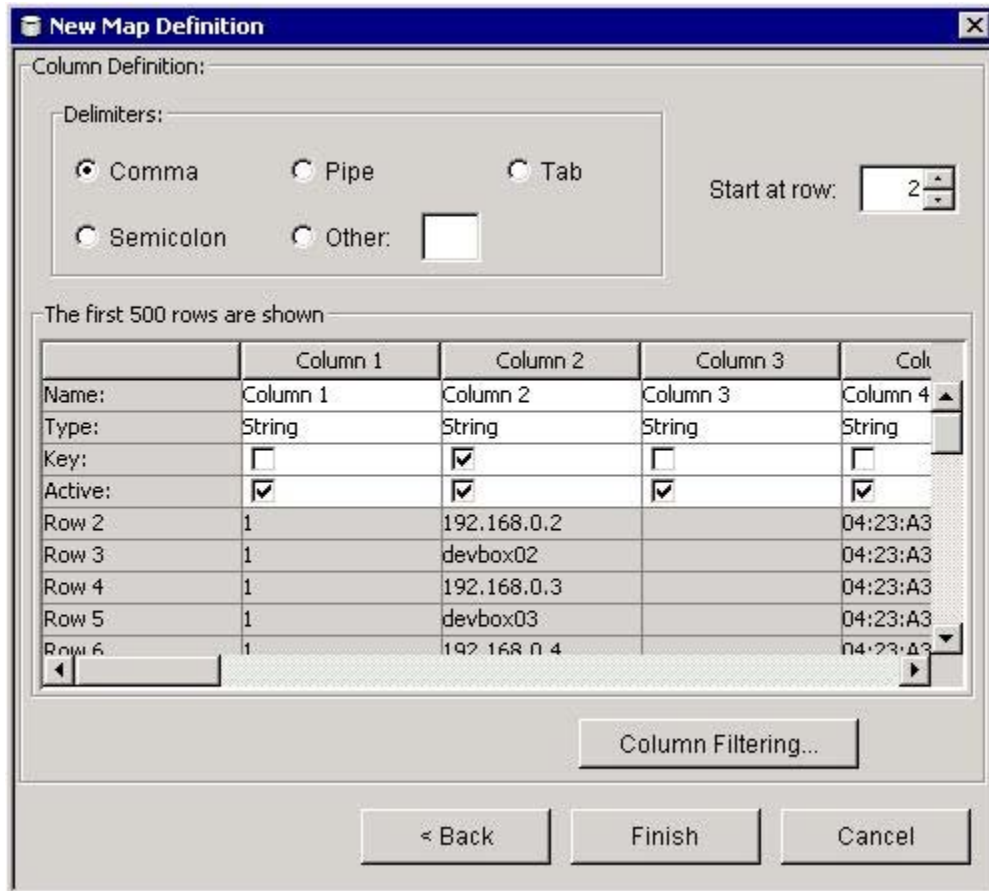
---

8. Nella finestra Nuova definizione mappatura, impostare quanto segue:
   - Delimitatore (barra verticale, virgola, punto e virgola e così via) dei dati nelle righe del file di origine dei dati di mappatura
   - Inizio alla riga: il numero di righe da ignorare a partire dall'inizio del file di origine dei dati di mappatura.
   - Nomi delle colonne
   - Tipi di colonna: i tipi di colonna attualmente supportati sono:
     - *Stringa:* una stringa è costituita da un gruppo di caratteri utilizzati come oggetto singolo da un computer. Le stringhe possono essere composta da una sola lettera, da una parola o da un numero. La parola FINANZA o l'indirizzo IP 192.168.2.40

sono esempi di stringhe. Le stringhe possono inoltre essere costituita da una combinazione di parole, spazi e numeri. L'indirizzo 1313 LION DOG TOWER è ad esempio una stringa di questo tipo.

  – *Intervallo numerico:* un intervallo numerico (NumberRange) è un intervallo di numeri. Ad esempio, l'intervallo compreso tra 10 e 200 verrebbe rappresentato come 10-200. Per utilizzare le funzionalità delle mappature di intervalli, la definizione della mappatura deve prevedere una sola colonna chiave la quale deve essere di tipo intervallo numerico. Se sono presenti altre colonne chiave o la colonna è di tipo diverso, il servizio di mappatura non considererà la mappatura come di intervalli.

- Colonne attive: se una colonna è contrassegnata come attiva, i suoi dati verranno distribuiti ai processi mediante le mappature. Tutte le colonne chiave devono essere attive. È possibile selezionare come “Colonna mappatura” nella scheda Eventi solo le colonne non chiave attive.
- Colonne chiave: si tratta di un identificatore univoco per la riga di dati nell'ambito dei dati di mappatura. Se sono selezionate come chiave più colonne, queste ultime costituiranno la chiave complessiva della mappatura.
- Filtri colonne: è possibile includere o escludere una riga in modo esplicito in base a criteri di corrispondenza relativi a una determinata colonna. In questo modo è possibile escludere le righe dai dati di origine della mappatura non necessari o che interferiscono con la mappatura.

La tabella dei dati verrà automaticamente aggiornata in conseguenza delle impostazioni e dei filtri di volta in volta configurati, in modo da consentire la visualizzazione dell'anteprima dei dati e di verificare che questi ultimi siano analizzati nel modo previsto.

9. Al termine della configurazione di tutti i parametri e i filtri per la definizione, fare clic su *Fine*.
10. Se nel passaggio 7 si sceglie File locale, verrà richiesto di caricare il file nella cartella virtuale dei file remoti che si trova in: %ESEC_HOME%\sentinel\bin\map_data. Immettere un nome per il file e fare clic su *OK*.

Aggiunta di definizioni di mappatura con intervallo numerico

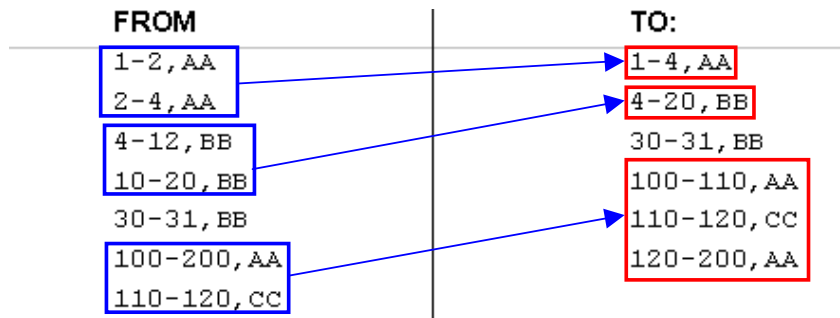
Per utilizzare le funzionalità delle mappature di intervalli, la definizione della mappatura deve prevedere una sola colonna chiave la quale deve essere di tipo intervallo numerico. Se sono presenti altre colonne chiave o la colonna è di tipo diverso, il servizio di mappatura non considererà la mappatura come di intervalli.

Per creare una mappa di intervalli, designare una sola colonna come chiave della mappatura e impostare il tipo come *intervallo numerico*. Il formato dei dati in una colonna di tipo *intervallo numerico* deve essere 'm-n' dove m è il numero minimo dell'intervallo e n il numero massimo, ad esempio 10-200. Il numero massimo non è incluso nell'intervallo, ovvero [m,n. Ciò significa che se si imposta l'intervallo 10-200 verranno considerati solo i numeri da 10 a 199. Un set di dati di esempio prevede la prima colonna impostata come chiave:

```
1-2,AA
2-4,AA
4-12,BB
10-20,BB
30-31,BB
100-200,AA
110-120,CC
```

The first 500 rows are shown

	Column 1	Column 2
Name:	Range	Value
Type:	NumberRange	String
Key:	☑	☐
Active:	☑	☑
Row 0	1-4	AA
Row 1	4-20	BB
Row 2	30-31	BB
Row 3	100-110	AA
Row 4	110-120	CC
Row 5	120-200	AA

Si noti la trasformazione della tabella nell'esempio.

Una configurazione di evento di esempio sulla mappatura sopra illustrata potrebbe essere la seguente:

È previsto che CustomerVar97 contenga un valore numerico oppure convertibile in valore numerico, ad esempio un indirizzo IP o una data.

Quando si eseguono ricerche nella mappatura di intervalli di esempio, il valore di CustomerVar97 prenderà in considerazione la mappatura di intervalli e cercherà l'intervallo a

cui appartiene il valore, se presente. Di seguito sono riportati alcuni esempi con i relativi risultati:

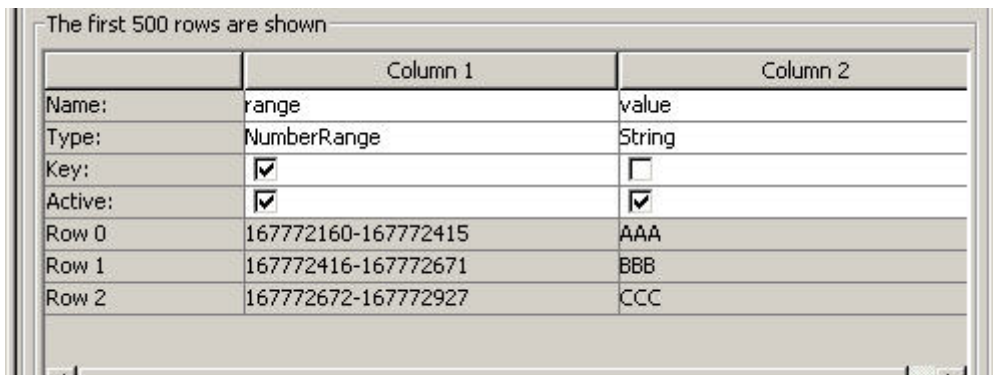
```
CustomerVar97 = 1; CustomerVar89 verrà impostato su AA
CustomerVar97 = 4; CustomerVar89 verrà impostato su BB
CustomerVar97 = 300; CustomerVar89 non verrà impostato
```

Sentinel converte internamente gli indirizzi IP e le date in un valore intero per i tag di tipo IPv4 e data.

I tag IPv4 sono:

- DestinationIP (IP di destinazione) - dip
- SourceIP (IP di origine) - sip

I tag di tipo data sono:

- Da CustomerVar11 a CustomerVar20 (da cv11 a cv20)
- DateTime (dt)
- Da ReservedVar11 a ReservedVar20 (da rv11 a rv20)

Per ulteriori informazioni sui tag META, vedere il capitolo 5 relativo a Wizard e ai tag META di Sentinel nella Guida di riferimento.

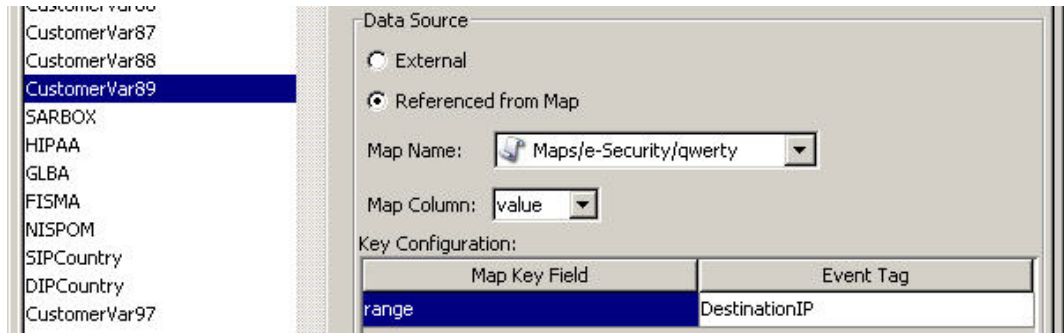
Nella tabella sottostante, ad esempio, la colonna 1 è un intervallo numerico equivalente a un intervallo di indirizzi IP compreso tra 10.0.0.0 e 10.0.2.255.

```
167772160-167772415,AAA
167772416-167772671,BBB
167772672-167772927,CCC
```

Utilizzando la stessa configurazione dell'esempio precedente, se:

- il tag di evento è impostato su DestinationIP e la colonna chiave sulla colonna 1 (intervallo)
- La colonna di mappatura sulla colonna 2 (valore). I valori di output per CustomerVar89.

The first 500 rows are shown

	Column 1	Column 2
Name:	range	value
Type:	NumberRange	String
Key:	☑	☐
Active:	☑	☑
Row 0	167772160-167772415	AAA
Row 1	167772416-167772671	BBB
Row 2	167772672-167772927	CCC

Se un evento contiene un IP di destinazione corrispondente a 10.0.1.14 (equivalente al valore numerico 167772430), l'output per la colonna CustomerVar89 nell'evento è BBB.

Sentinel supporta gli intervalli numerici seguenti:

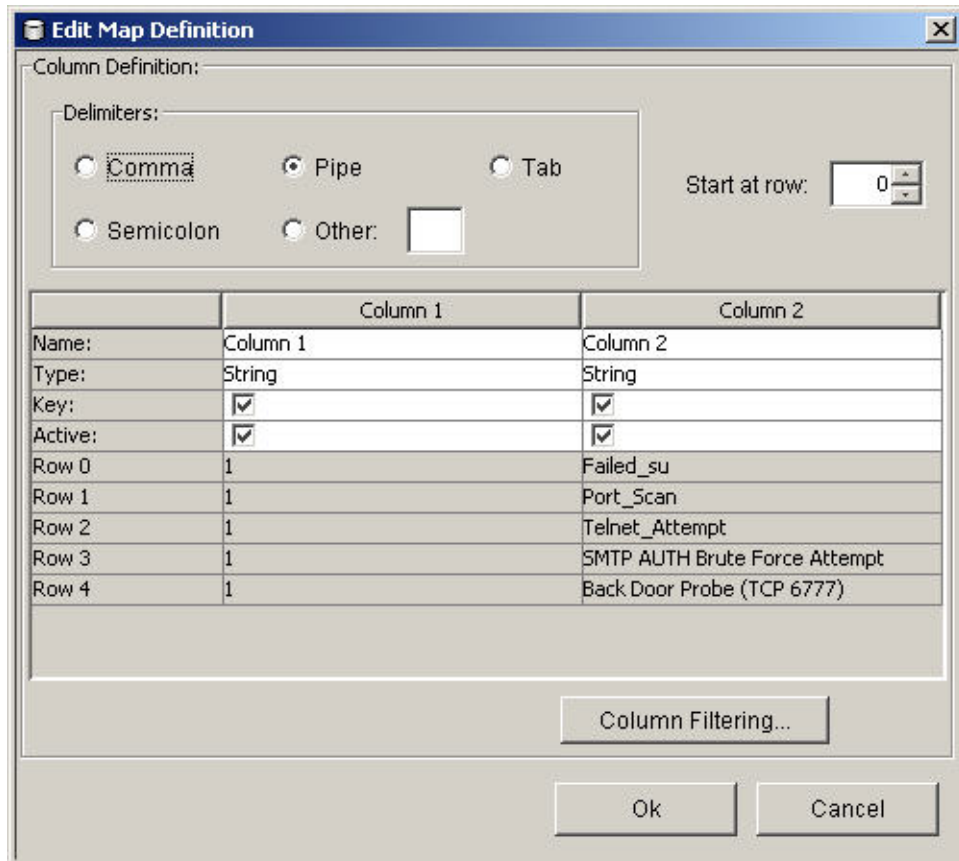
- Intervallo tra numeri negativi (ad esempio "-234--34")
- Intervallo tra un numero negativo e un numero positivo (ad esempio "-234-34")
- Intervallo tra numeri positivi (ad esempio "234-236")
- Intervallo costituito da un solo numero negativo, ad esempio "-234". In questo caso il minimo e il massimo saranno entrambi -234.
- Intervallo costituito da un solo numero positivo, ad esempio "234". In questo caso il minimo e il massimo saranno entrambi 234.
- Intervallo tra un numero negativo e un numero massimo (ad esempio "-234-") In questo caso il minimo sarà -234 e il massimo sarà (2^63 - 1).
- Intervallo tra un numero positivo e un numero massimo (ad esempio "-234-") In questo caso il minimo sarà 234 e il massimo sarà (2^63 - 1).

NOTA: In tutti i casi, il minimo deve essere minore o uguale al massimo (ad esempio "-234—235" non è valido).

Modifica delle definizioni di mappatura

Per modificare una definizione di mappatura:

1. Fare clic sulla scheda *Mappatura*.
2. Espandere la cartella desiderata.
3. Evidenziare una definizione di mappatura e fare clic sul pulsante *Modifica*.

NOTA: La funzione di modifica è disabilitata per le definizioni di mappatura che si trovano nella cartella System.

La funzione di modifica consente di:

- impostare i delimitatori
- impostare la riga iniziale della mappatura
- rinominare le colonne
- attivare o disattivare una colonna
- impostare le colonne chiave
- filtrare le colonne

4. Al termine, fare clic su *OK*.

Eliminazione delle definizioni di mappatura

Per eliminare una definizione di mappatura

1. Fare clic sulla scheda Mappatura.
2. Espandere la cartella desiderata.
3. Evidenziare la definizione di mappatura da eliminare.
4. Fare clic su *Elimina*.

NOTA: Non è possibile eliminare le definizioni di mappatura nella cartella Sentinel.

Aggiornamento dei dati di mappatura

L'aggiornamento consente di sostituire il file dei dati di origine di una mappatura sul server che esegue DAS con un altro file. Affinché la mappatura aggiornata funzioni correttamente, nel nuovo file dei dati di origine della mappatura devono essere impostati lo stesso delimitatore, lo stesso numero di colonne e la stessa struttura generale del file esistente. L'unica differenza consentita tra il nuovo file dei dati di origine della mappatura e quello

esistente è quella tra i valori delle colonne. Se il nuovo file di dati di origine della mappatura ha una struttura diversa rispetto al file esistente, utilizzare la funzione Modifica dell'interfaccia utente grafica di Gestione dati Sentinel per aggiornare la definizione di mappatura.

Per aggiornare i dati di mappatura

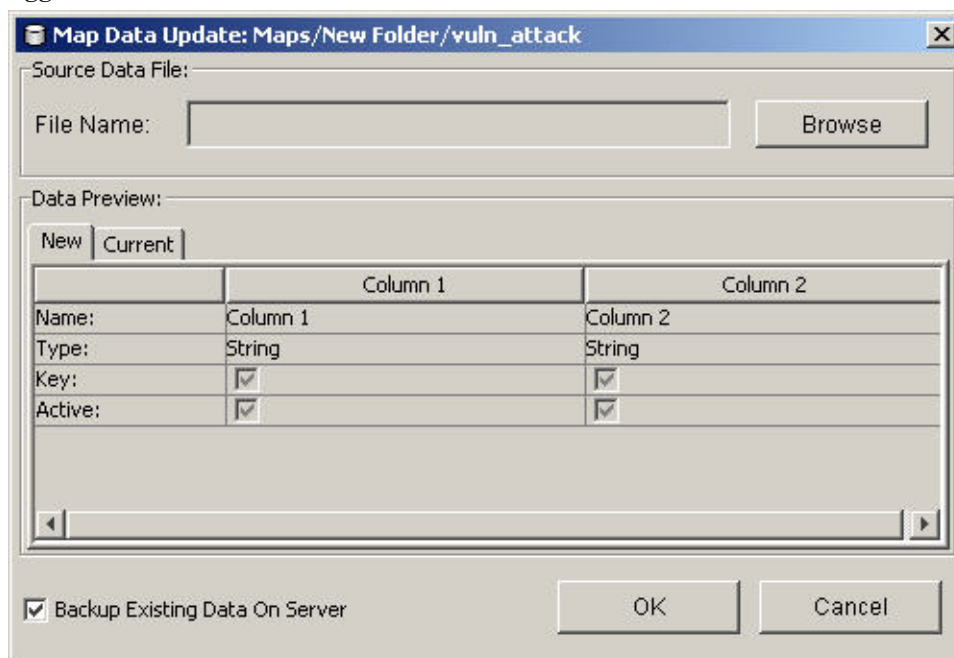
1. Se non è già stato fatto, creare un file contenente i nuovi dati di origine della mappatura nel computer che esegue Gestione dati Sentinel. Il file può essere generato, ad esempio da uno script di dump dei dati, creato manualmente da zero oppure consistere in una versione modificata del file di origine dei dati di mappatura esistente. Se necessario, è possibile ottenere il file di origine dei dati di mappatura dall'ubicazione indicata di seguito:

   Per Windows:

   ```
   %ESEC_HOME%\sentinel\bin\map_data
   ```

   Per UNIX:

   ```
   $ESEC_HOME/sentinel/bin/map_data
   ```

2. Fare clic sulla scheda *Mappatura*.
3. Espandere la cartella desiderata. Evidenziare la mappatura da aggiornare. Fare clic su *Aggiorna*.

4. Selezionare il nuovo file di origine della mappatura facendo clic sul pulsante Sfoglia e selezionando il file con i nuovi dati di mappatura. Dopo aver selezionato il file, i relativi dati di mappatura verranno visualizzati nella scheda *Nuovo*. I dati di mappatura da sostituire verranno visualizzati nella scheda Attuale.
5. Deselezionare o lasciare l'impostazione di default per "*Esegui backup dei dati esistenti sul server*". Se si abilita questa opzione, verrà creata una copia di backup del file di origine dei dati di mappatura esistente, la quale verrà inserita nella cartella %ESEC_HOME%\sentinel\bin\map_data (Windows) o

$ESEC_HOME/sentinel/bin/map_data (UNIX). Il prefisso del nome del file di origine dei dati di mappatura corrisponderà a quello del file esistente. Al nome del file verrà accodata una serie di numeri casuale seguita dal suffisso .bak. Ad esempio: vuln_attacks10197.bak.

6. Fare clic su *OK*.
7. I dati del nuovo file di origine dei dati di mappatura verranno caricati sul server per sostituire i contenuti del file esistente. Al termine del caricamento dei dati di origine, i dati di mappatura verranno rigenerati e distribuiti ai client di mappatura, ad esempio Gestione servizi di raccolta.

Scheda Eventti

NOTA: Per utilizzare la scheda Eventi, è necessario che il file configuration.xml faccia riferimento a un'istanza di Communication Server connessa inoltre a DAS_Binary e DAS_Query. Si tratta in genere della situazione di default purché Communication Server e i processi DAS siano in esecuzione.

Mappatura di eventi

La mappatura degli eventi è un meccanismo che consente di aggiungere dati a un evento utilizzando i dati già presenti nell'evento per fare riferimento a quelli di un'origine esterna ed estrarli. L'origine dati esterna consiste in una mappatura definita mediante la scheda Mappatura. I dati già presenti nell'evento da utilizzare come riferimento nella mappatura e i dati da estrarre dalla mappatura nell'evento vengono specificati nella scheda Eventi.

Poiché in una mappatura può essere creato qualsiasi set di dati, la mappatura degli eventi risulta utile per incorporare nel flusso di eventi dati provenienti da qualsiasi posizione nell'organizzazione. Alcune funzionalità offerte dalla mappatura di eventi sono:

- Il monitoraggio della conformità alle normative
- La conformità ai criteri
- La priorità delle risposte
- L'abilitazione dei dati di sicurezza da analizzare in relazione alle attività aziendali
- L'ottimizzazione della contabilità

Quando si definisce una mappatura di eventi, quest'ultima viene applicata a livello di sistema a tutti gli eventi di tutti i servizi di raccolta. Sentinel distribuirà inoltre automaticamente i dati di mappatura a tutti i processi che eseguono mappature di eventi e manterrà aggiornati i dati di mappatura in tali processi. La mappatura di eventi offre pertanto importanti funzionalità per il supporto delle distribuzioni aziendali.

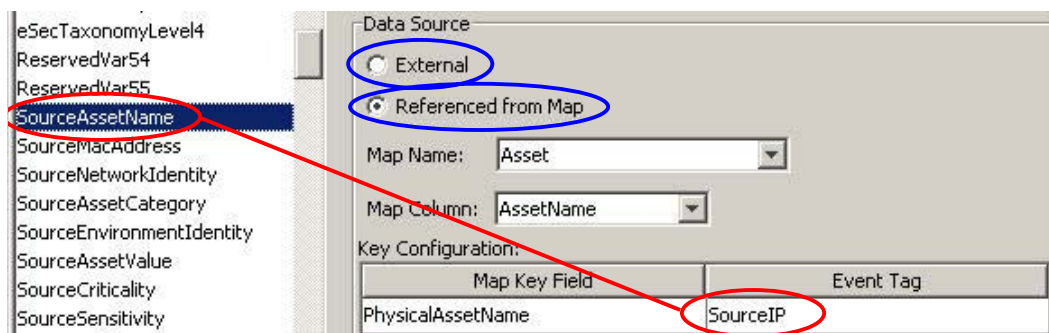
La mappatura di eventi è costituita da quattro parti principali:

- Controller, che memorizza tutte le informazioni di mappatura
- Server di distribuzione, che ridistribuisce automaticamente le mappature modificate nei processi registrati per la mappatura
- Monitoraggio, che consente di rilevare le modifiche apportate ai dati di mappatura
- Generatore, che genera le mappature a partire dai dati di origine

Un'applicazione della mappatura di eventi è rappresentata dalla funzionalità Dati risorsa di Sentinel. Le informazioni sulle risorse vengono ad esempio raccolte e memorizzate nello schema delle risorse del database di Sentinel e rappresentate da una voce di risorsa fisica. Risorse software, ad esempio servizi e applicazioni, vengono rappresentate da una voce collegata a una risorsa fisica. Il meccanismo di aggiornamento automatico principale dei dati

delle risorse prevede la lettura dei dati da parte di un servizio di raccolta delle risorse mediante un servizio di scansione, ad esempio Nmap. Il servizio di raccolta consente di automatizzare il recupero delle informazioni sulle risorse tramite la lettura dei relativi dati dal servizio di scansione e il popolamento delle tabelle dello schema delle risorse con tali dati. Ai fini della mappatura di eventi, le informazioni sulle risorse vengono mappate in base all'IP di destinazione e a quello di origine.

Esistono due tipi di origini dati:

- Esterna: un servizio di raccolta inserisce il valore nel tag di evento.
- Riferimento da mappatura: i dati vengono recuperati da una mappatura al fine di popolare il tag.

Nell'illustrazione riportata sopra, il tag SourceAssetName viene popolato a partire dalla mappatura denominata Asset il cui file di origine dei dati di mappatura è asset.csv. Il valore specifico relativo a SourceAssetName deriva dalla colonna AssetName della mappatura Asset. La colonna PhysicalAssetName è impostata come chiave. Se il tag SourceIP dell'evento corrisponde a uno dei valori di IP di origine nella colonna PhysicalAssetName della mappatura, la riga con la chiave corrispondente verrà utilizzata per l'intersezione con la colonna AssetName. Nell'esempio seguente l'IP 198.168.1.100 corrisponde ad esempio al valore Finance35 di AssetName.

NOTA: Se una colonna è imposta come chiave, non verrà visualizzata nel campo a discesa Colonna.

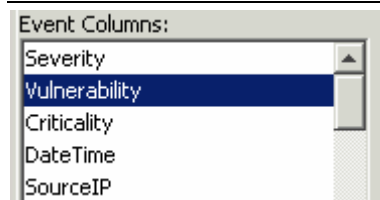
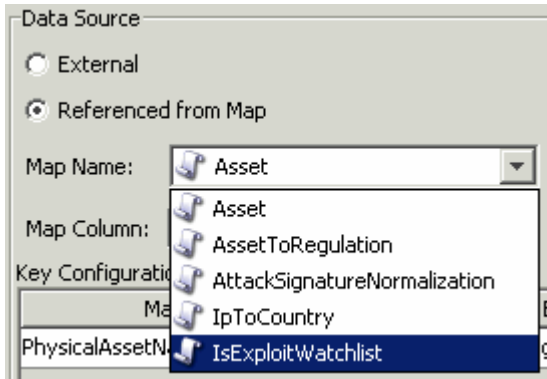
PhysicalAssetName	CustomerID	MacAddress	AssetName
198.168.1.91			Marketing01
198.168.1.95			Marketing02
198.168.1.96			ProgramMgmt03
198.168.1.98			Finance34
198.168.1.100			Finance35

È possibile disporre di più colonne impostate come chiave qualora non si desideri una mappatura di intervalli. In questo tipo di mappatura è possibile impostare una sola colonna chiave di tipo intervallo numerico. Ad esempio, con una colonna di tipo stringa, per il tag AttackId le colonne DeviceName (nome del dispositivo di sicurezza) e DeviceAttackName sono impostate come chiave e viene utilizzata la colonna NormalizedAttackID nella mappatura AttackNormalization per ottenerne il valore. In una riga in cui il tag di evento DeviceName corrisponde ai dati nella colonna di mappatura Device e DeviceAttackName corrisponde ai dati nella colonna di mappatura AttackSignature, il valore relativo ad AttackId

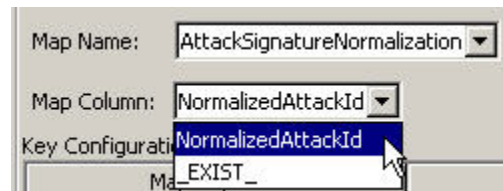
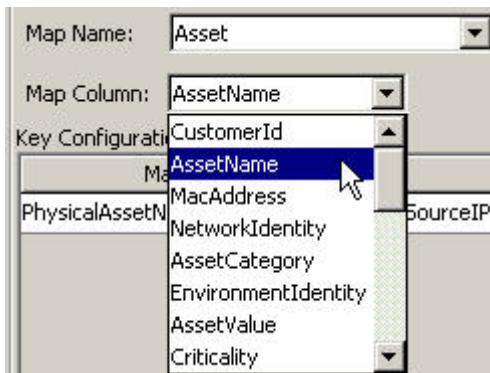
corrisponde a quello nella colonna NormalizedAttackID. La configurazione relativa alla mappatura di eventi appena descritta è:

Configurazione dei tag di evento (colonne) per utilizzare la mappatura

1. Fare clic sulla scheda *Eventi*.
2. Evidenziare una voce di tag di evento nell'elenco Colonne evento.

NOTA: Il nome del tag di evento originale viene visualizzato sul campo Etichetta. Viene inoltre fornita la descrizione della colonna degli eventi.

3. Fare clic su “Riferimento da mappatura” per configurare il tag di evento in modo che venga popolato con i dati di una mappatura. Fare clic su Esterna per mantenere qualsiasi eventuale valore venga inserito nel tag di evento dal servizio di raccolta.
4. Fare clic sul campo a discesa *Nome della mappatura*.

Selezionare una delle mappature di default seguenti oppure una creata dall'utente:

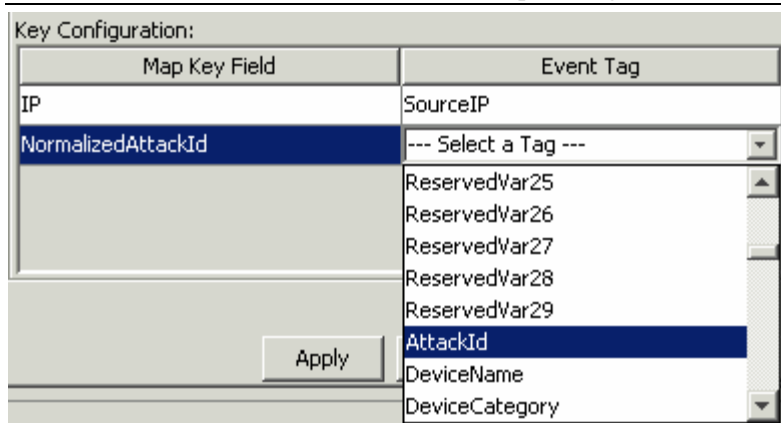
- Risorsa: contiene i dati del file di origine dei dati di mappatura asset.csv. Il file asset.csv viene generato automaticamente in base ai dati di risorsa di un database di Sentinel al momento dell'esecuzione di un servizio di raccolta delle risorse. Se lo si desidera, è possibile popolare questo file manualmente.
- AssetToRegulation: contiene i dati del file di origine dei dati di mappatura AssetToRegulation.csv. È necessario popolare questo file manualmente.
- AttackSignatureNormalization: contiene i dati del file di origine dei dati di mappatura attackNormalization.csv (firme IDS). Il file attackNormalization.csv viene generato automaticamente in base ai dati di Advisor di un database di Sentinel al completamento di un feed di Advisor.
- IpToCountry: contiene i dati del file di origine dei dati di mappatura IpToCountry.csv. È necessario popolare questo file manualmente.
- IsExploitWatchlist: contiene i dati del file di origine dei dati di mappatura exploitDetection.csv (vulnerabilità e minacce). Il file exploitDetection.csv viene generato automaticamente in base ai dati di Advisor e di vulnerabilità di un database di Sentinel al completamento di un feed di Advisor oppure al momento dell'esecuzione di un servizio di raccolta di vulnerabilità..

5. Fare clic sul campo a discesa *Mappatura colonna* e selezionare un nome di *colonna di mappatura*. I valori disponibili dipendono dalla scelta effettuata nel passaggio precedente.

- _EXIST_: si tratta di una colonna di mappatura speciale esistente in tutte le mappature. Se si seleziona questa colonna di mappatura, nel tag di evento verrà

inserito il valore “1” se la chiave è inclusa nei dati di mappatura. In caso contrario, nel tag di evento verrà inserito il valore “0”.

- Tutte le altre opzioni: i nomi di colonne attive nella definizione di mappatura non impostate come chiave (ad esempio la colonna CustomerId in Asset oppure la colonna NormalizedAttackId in AttackNormalization)

6. In Configurazione chiave, per ogni riga nella tabella selezionare il tag di evento nella colonna Tag evento i cui valori corrisponderanno alla colonna chiave della mappatura specificata nella colonna Campo chiave per mappatura corrispondente. Le righe disponibili nella tabella Configurazione chiave dipendono dal nome della mappatura selezionato.

NOTA: Le chiavi sono identificatori univoci per la riga dei dati di mappatura.

7. Fare clic su *Applica*.

NOTA: Se si fa clic su *Applica*, le modifiche apportante alla colonna di evento attualmente selezionata verranno salvate in un buffer temporaneo. Se non si fa clic su *Applica* e si seleziona un'altra colonna di evento, le modifiche apportate alla colonna di evento selezionata precedentemente verranno perse. Le modifiche verranno salvate nel server solo dopo aver fatto clic su *Salva*.

8. Se si desidera modificare la *mappatura di evento* di un'altra colonna di evento, ripetere i passaggi descritti sopra. Accertarsi di fare clic su *Applica* dopo avere apportato le modifiche alla *mappatura di evento* di ogni colonna di evento.
9. Fare clic su *Salva*.

NOTA: Se si fa clic su *Salva*, le modifiche verranno salvate sul server. La funzione di salvataggio consente di salvare tutte le modifiche memorizzate nel buffer temporaneo (dopo aver fatto clic su *Applica*).

Ridenominazione di tag

La scheda Eventi consente inoltre di assegnare nomi a etichette di tag di evento esistenti. È ad esempio possibile rinominare l'etichetta relativa al tag di evento Ct2 in City. In questo modo il tag “Ct2” verrà visualizzato in Sentinel Control Center come “City”. I tag di evento sono presenti in posizioni di Sentinel Control Center quali filtri, regole di correlazione e visualizzazioni Active Views.

La ridenominazione dei tag non modifica tuttavia la variabile negli script del servizio di raccolta. Pertanto, anche se l'evento con etichetta Ct2 viene rinominato City, la variabile da

utilizzare in uno script del servizio di raccolta per fare riferimento a tale tag META deve essere comunque s_CT2.

Nella figura seguente viene illustrato l'effetto di questa funzione in una visualizzazione Active Views.

Istantanea PUBLIC:High_Severity @ 07/07/06 17.36.28

urceIP	DestinationIP	EventName	Ct2	Vulnerability	Criticality
	172.16.5.104	Reject	Cupertino	0	7
	172.16.2.105	Reject	Orlando	0	7
	172.16.2.105	Reject	Orlando	0	7
	172.16.5.105	Reject	Cupertino	0	7
	172.16.2.106	Reject	Orlando	0	7
	172.16.2.106	Reject	Orlando	0	7
59	172.16.2.105	SSH exploit attempt	Orlando	0	7
	172.16.7.105	Reject	Chicago	0	4

Istantanea PUBLIC:High_Severity @ 07/07/06 17.36.28

urceIP	DestinationIP	EventName	City	Vulnerability	Criticality
	172.16.5.104	Reject	Cupertino	0	7
	172.16.2.105	Reject	Orlando	0	7
	172.16.2.105	Reject	Orlando	0	7
	172.16.5.105	Reject	Cupertino	0	7
	172.16.2.106	Reject	Orlando	0	7
	172.16.2.106	Reject	Orlando	0	7
59	172.16.2.105	SSH exploit attempt	Orlando	0	7
	172.16.7.105	Reject	Chicago	0	4

Ridenominazione di una colonna di evento

1. Fare clic sulla scheda *Eventi*.

   NOTA: Il nome della colonna di evento originale viene visualizzato sul campo Etichetta. Viene inoltre fornita la descrizione della colonna degli eventi.

2. Evidenziare una voce di colonna di evento.
3. Immettere un nuovo valore per la colonna di evento nel campo Etichetta.

4. Fare clic su *Applica*.

   NOTA: Se si fa clic su *Applica*, le modifiche apportate al tag di evento attualmente selezionato verranno salvate in un buffer temporaneo. Se non si fa clic su *Applica* e si seleziona un altro tag di evento, le modifiche apportate al tag di evento selezionato precedentemente verranno perse. Le modifiche verranno salvate nel server solo dopo aver fatto clic su *Salva*.

5. Fare clic su *Salva*.

   NOTA: Se si fa clic su *Salva*, le modifiche verranno salvate sul server. La funzione di salvataggio consente di salvare tutte le modifiche memorizzate nel buffer temporaneo (dopo aver fatto clic su *Applica*).

6. Affinché le modifiche vengano visualizzate in Sentinel Control Center, quest'ultimo deve essere chiuso e quindi riavviato.

Scheda Rapporto dati

NOTA: Per utilizzare la scheda Rapporto dati, è necessario che il file configuration.xml faccia riferimento a un'istanza di Communication Server connessa inoltre a DAS_Binary e DAS_Query. Si tratta in genere della situazione di default purché Communication Server e i processi DAS siano in esecuzione.

La scheda *Rapporto dati* costituisce l'interfaccia di gestione di riepilogo per Sentinel. Questa scheda consente di abilitare e disabilitare i **riepiloghi**. In questo modo il componente Aggregazione potrà avviare il calcolo dei totali relativi a un determinato riepilogo.

I riepiloghi sono gruppi definiti di attributi che costituiscono la chiave per la quale viene calcolato il numero di occorrenze univoche (numero di eventi) in un determinato periodo di tempo espresso in ore (orario evento). Nel caso di *EventSevDestPortSummary*, se *attivo*, viene salvato il numero di eventi per ogni combinazione univoca di porta di destinazione e gravità relativamente a un determinato orario. I calcoli salvati dei dati di evento consentono di generare rapporti ed effettuare interrogazioni sui riepiloghi in modo più rapido. I rapporti vengono utilizzati da Crystal Reports. Per ulteriori informazioni, vedere il capitolo relativo all'installazione di Crystal Reports nella Guida all'installazione. Affinché i rapporti relativi ad determinati riepiloghi risultino precisi, è necessario che questi ultimi siano “attivi”.

L'aggregazione è il processo di calcolo del numero di esecuzioni relative a tutti i riepiloghi attivi durante il flusso di eventi attraverso il sistema. I numeri di esecuzioni vengono salvati nel database nelle rispettive tabelle di riepilogo.

Vantaggi dei riepiloghi:

- Notevole riduzione dei gruppi di dati di evento
- Dimensioni conformi che consentono di eseguire il drill-down, il rollup e il drill-across dei dati degli eventi
- Esecuzione di rapporti sui riepiloghi precalcolati notevolmente più veloce

Vantaggi dell'aggregazione:

- Elaborazione dei soli riepiloghi attivi
- Assenza di effetti sull'inserimento di eventi nel database in tempo reale

La scheda Rapporto dati consente di:

- abilitare/disabilitare eventuali riepiloghi predefiniti
- visualizzare gli attributi di ogni riepilogo
- verificare la validità di un riepilogo in un determinato periodo di tempo
- individuare i *file di evento* che devono essere eseguiti per il completamento del riepilogo.

Nella tabella seguente vengono indicati riepiloghi già definiti nel sistema. Vengono indicati il nome del riepilogo, il nome della tabella del database e i relativi attributi in una breve descrizione del riepilogo stesso.

Nome riepilogo	Tabella/descrizione
EventSrcSummary	EVT_SRC_SMRY_1 Questo riepilogo somma il numero di eventi in base a IP di origine, informazioni sulla risorsa di origine, porta di origine, utente di origine, tassonomia, nome di evento, risorsa, servizio di raccolta, protocollo, gravità e orario evento per ora
EventDestSummary	EVT_DEST_SMRY_1 Questo riepilogo somma il numero di eventi in base a IP di destinazione, informazioni sulla risorsa di destinazione, porta di destinazione, utente di destinazione, tassonomia, nome di evento, risorsa, servizio di raccolta, protocollo, gravità e orario evento per ora
EventSevDestTxnmySummary	EVT_ DEST_TXNMY_SMRY_1 Questo riepilogo somma il numero di eventi in base a IP di destinazione, informazioni sulla risorsa di destinazione, tassonomia, gravità e orario evento per ora
EventSevDestEvtSummary	EVT_DEST_EVT_NAME_SMRY_1 Questo riepilogo somma il numero di eventi in base a IP di destinazione, risorsa dell'evento di destinazione, tassonomia, nome evento, gravità e orario evento per ora
EventSevDestPortSummary	EVT_PORT_SMRY_1 Questo riepilogo somma il numero di eventi in base a porta di destinazione, gravità e orario evento per ora
EventSevSummary	EVT_SEV_SMRY_1 Questo riepilogo somma il numero di eventi in base a gravità e orario evento per ora

Disabilitazione/abilitazione di un riepilogo

1. Fare clic sulla scheda *Rapporto dati*.
2. Per disabilitare un riepilogo, fare clic sul pulsante “*Attiva*” nella colonna Stato in modo da impostare lo stato su “*Disattivo*”.
3. Per disabilitare un riepilogo, fare clic sul pulsante “*Attiva*” nella colonna Stato in modo da impostare lo stato su “*Disattivo*”.

Per abilitare *l'aggregazione per i primi 10 report* di Crystal Reports:

- Abilitare i tre riepiloghi seguenti:
  - EventDestSummary
  - EventSevSummary
  - EventSrcSummary

- Abilitare EventFileRedirectService nel file das_binary.xml che si trova in:

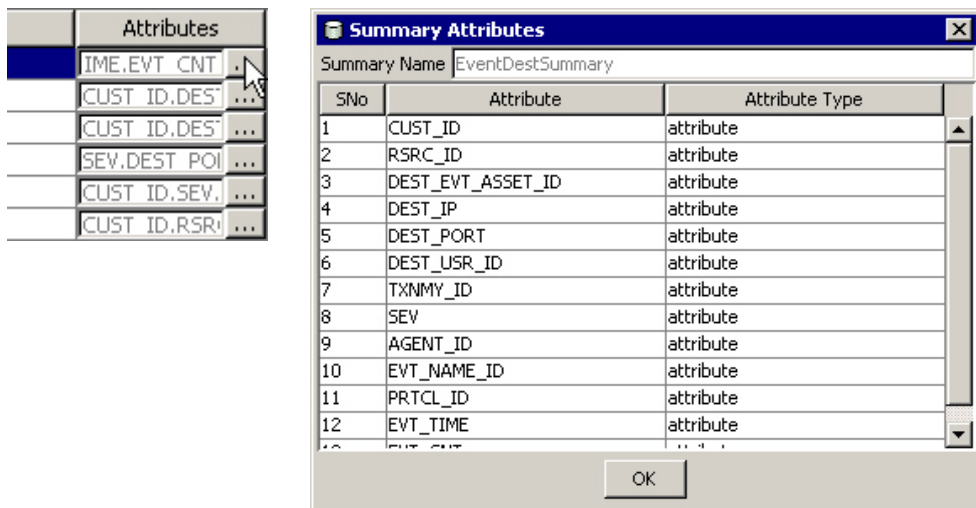
Per UNIX:

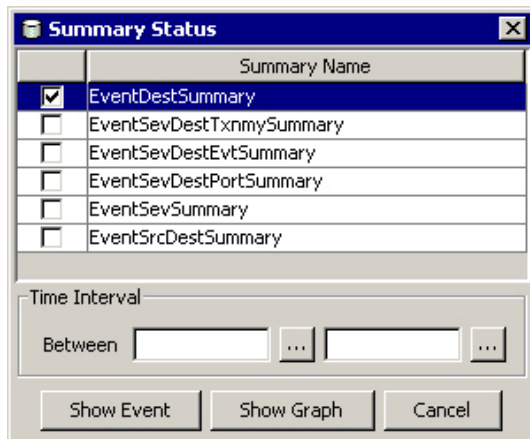
```
$ESEC_HOME/sentinel/config/das_binary.xml
```

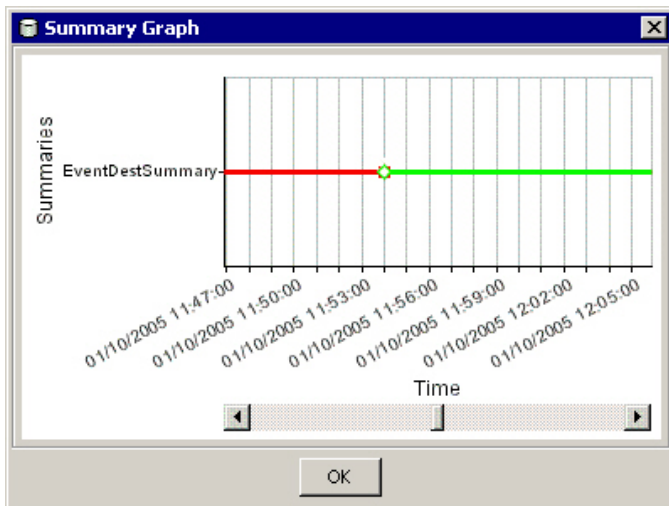
Per Windows:

```
%ESEC_HOME%\sentinel\config\das_binary.xml
```

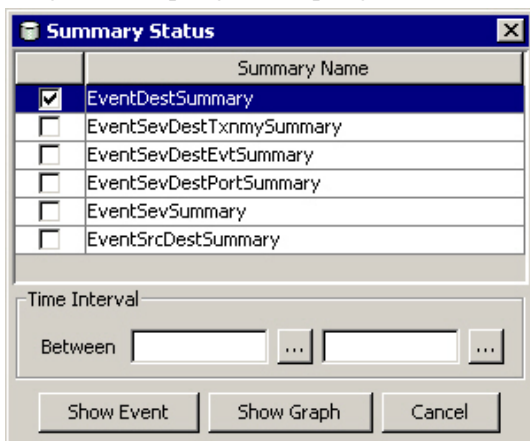
Visualizzazione di informazioni relative a un riepilogo

1. Fare clic sulla scheda *Rapporto dati*.
2. Fare clic sul pulsante "…" nella colonna Attributi per visualizzare gli attributi che costituiscono il riepilogo.

Verifica della validità di un riepilogo

1. Fare clic sulla scheda *Rapporto dati*.
2. Selezionare *Stato*.
3. Scegliere il riepilogo o i riepiloghi su cui si desidera eseguire l'interrogazione.

4. Selezionare un intervallo di tempo.
5. Fare clic su *Mostra grafico*.

6. Le barre verdi indicano che il riepilogo è completo per il periodo di tempo specificato. Le sezioni di colore rosso indicano l'assenza di dati nel riepilogo durante il periodo di tempo indicato.

NOTA: Per completare i riepiloghi, vedere *la sezione relativa all'esecuzione di Event Files per un riepilogo*.

Interrogazione di EventFiles per un riepilogo

1. Fare clic sulla scheda *Rapporto dati*.
2. Selezionare *Stato*.
3. Scegliere il riepilogo o i riepiloghi su cui si desidera eseguire l'interrogazione.

4. Selezionare un intervallo di tempo.
5. Fare clic su *Mostra evento*.
6. I file di evento necessari per completare il riepilogo vengono visualizzati sotto forma di elenco.

NOTA: Per completare i riepiloghi, vedere *la sezione relativa all'esecuzione di Event Files per un riepilogo*.

Processed Summary Status

	Summary	File Name	Min Event Time	Max Event Time	Process
1	EventDestSummary	events_20050110_1...	Mon Jan 10 13:27:02 EST...	Mon Jan 10 13:57:02 EST 2005	☐
2	EventDestSummary	events_20050110_1...	Mon Jan 10 13:57:03 EST...	Mon Jan 10 14:27:03 EST 2005	☐
3	EventDestSummary	events_20050110_1...	Mon Jan 10 14:27:53 EST...	Mon Jan 10 14:43:12 EST 2005	☐
4	EventDestSummary	events_20050110_1...	Mon Jan 10 14:48:25 EST...	Mon Jan 10 15:19:17 EST 2005	☐
5	EventDestSummary	events_20050110_1...	Mon Jan 10 15:15:17 EST...	Mon Jan 10 23:44:00 EST 2005	☐
6	EventDestSummary	events_20050110_1...	Mon Jan 10 15:50:33 EST...	Mon Jan 10 16:20:33 EST 2005	☐
7	EventDestSummary	events_20050110_1...	Mon Jan 10 16:20:40 EST...	Mon Jan 10 16:50:40 EST 2005	☐
8	EventDestSummary	events_20050110_1...	Mon Jan 10 16:46:31 EST...	Mon Jan 10 17:20:40 EST 2005	☐
9	EventDestSummary	events_20050110_1...	Mon Jan 10 17:16:32 EST...	Mon Jan 10 17:50:40 EST 2005	☐
10	EventDestSummary	events_20050110_1...	Mon Jan 10 17:46:42 EST...	Mon Jan 10 18:20:49 EST 2005	☐
11	EventDestSummary	events_20050110_1...	Mon Jan 10 18:20:38 EST...	Mon Jan 10 18:50:40 EST 2005	☐
12	EventDestSummary	events_20050110_1...	Mon Jan 10 18:50:40 EST...	Mon Jan 10 19:20:41 EST 2005	☐
13	EventDestSummary	events_20050110_1...	Mon Jan 10 19:20:42 EST...	Mon Jan 10 19:50:43 EST 2005	☐
14	EventDestSummary	events_20050110_1...	Mon Jan 10 19:50:44 EST...	Mon Jan 10 20:20:44 EST 2005	☐
15	EventDestSummary	events_20050110_1...	Mon Jan 10 20:20:45 EST...	Mon Jan 10 20:50:46 EST 2005	☐
16	EventDestSummary	events_20050110_1...	Mon Jan 10 20:50:47 EST...	Mon Jan 10 21:20:46 EST 2005	☐
17	EventDestSummary	events_20050110_1...	Mon Jan 10 21:20:48 EST...	Mon Jan 10 21:50:49 EST 2005	☐

Process   Close

Esecuzione di Eventfiles per un riepilogo

1. Fare clic sulla scheda *Rapporto dati*.
2. Selezionare *Stato*.
3. Scegliere il *riepilogo* o i *riepiloghi* su cui si desidera eseguire l'interrogazione.
4. Selezionare un intervallo di tempo.
5. Fare clic su *Mostra evento*.
6. I file di *evento* necessari per completare il riepilogo vengono visualizzati sotto forma di elenco.
7. Selezionare i file di *evento* da eseguire per completare il riepilogo.

8. Fare clic su *Processo*.

Riga di comando di Gestione dati Sentinel

NOTA: Se con il computer in uso non è possibile accedere a DAS_Binary e DAS_Query, utilizzare la riga di comando di Gestione dati Sentinel anziché l'interfaccia utente.

Salvataggio di proprietà di connessione per Gestione dati Sentinel

Questa operazione deve essere eseguita prima di utilizzare qualsiasi operazione dalla riga di comando di Gestione dati Sentinel diversa da saveConnection.

Se è necessario eseguire l’interfaccia utente grafica di Gestione dati Sentinel, è possibile utilizzare il file sdm.connect creato dall’interfaccia utente grafica, il quale si trova in %ESEC_HOME%\sdm per Windows e in $ESEC_HOME/sdm per UNIX.

La funzione di salvataggio della connessione consente di salvare i dettagli seguenti insieme alla password cifrata (mediante l'archivio chiavi specificato in configuration.xml) nel file specificato.

Con questo comando vengono utilizzati i flag seguenti:

-action	saveConnection
-server	<oracle o mssql)>
-host	<indirizzo IP dell'host del database o nome host a cui connettersi>
-port	<numero di porta del database a cui connettersi [il valore di default per Oracle è: 1521/quello per SQL Server è: 1433]>
-database	<nome/SID del database a cui connettersi>
-user	<nome utente del database>
-password	<password del database>
-winAuth	utilizzato per l'autenticazione di Windows. Quando si utilizza questa opzione, non utilizzare -user e –password.
-connectFile	<nome del file scelto dall'utente in cui salvare i dettagli della connessione>

I dettagli di connessione in alto vengono salvati nel file specificato insieme alla password cifrata. Per eseguire gli altri comandi, l'applicazione utilizza i dettagli della connessione salvati. È necessario completare questo passaggio la prima volta che si avvia l'applicazione e ogni volta che si desidera modificare i dettagli della connessione.

Esecuzione di saveConnection

1. Eseguire il comando nel modo seguente:

```
sdm -action saveConnection -server <oracle/mssql> -
   host <hostIp/hostName> -port <portnum> -database
   <databaseName/SID> [-driverProps <propertiesFile>]
   {-user <dbUser> -password <dbPass> | -winAuth} -
   connectFile <filenameToSaveConnection>
```

   Nell'esempio seguente vengono salvati i dettagli della connessione relativi a un host con indirizzo IP 172.16.0.36 sulla porta 1521 (impostazione di default di Oracle, quella di SQL Server è 1433).

   - Esempio per Oracle:

```
./sdm -action saveConnection -server oracle -host
   172.16.0.36 -port 1521 -database esec -user esecdba
   -password XXXXXX -connectFile sdm.connect
```

   - Esempio per SQL Server:

```
sdm -action saveConnection -server mssql -host
   172.16.0.36 -port 1433 -database esec -user esecdba
   -password XXXXXX -connectFile  sdm.connect
```

   Nell'esempio seguente vengono salvati i dettagli della connessione relativi a un host con indirizzo IP 172.16.0.36 sulla porta 1433, con nome di database esec_51 per l'autenticazione di Windows.

- Esempio per SQL Server (autenticazione di Windows).

```
sdm -action saveConnection -server mssql -host
   172.16.1.3 -port 1433 -database esec_51 –winAuth -
   connectFile  %ESEC_HOME%\sdm\sdm.connect
```

I dettagli della connessione vengono salvati nel file sdm.connect. Tutti gli altri comandi utilizzano questo nome di file come input per effettuare la connessione al database specificato ed eseguire le relative azioni.

Gestione delle partizioni

Configurazione di partizioni

Si applica solo a Oracle. Questa azione (partitionConfig) viene utilizzata per configurare le partizioni del database in uso. Questa configurazione determina la modalità di aggiunta delle partizioni a tutte le tabelle partizionate di Sentinel. Con questa azione vengono utilizzati i flag seguenti:

-action	partitionConfig
-freq	<"3D" o "2D" o "1D" o 1W> Le uniche opzioni supportate sono: 3D: tre partizioni al giorno 2D: due partizioni al giorno 1D: una partizione al giorno 1W: una partizione alla settimana
-days	<numero di giorni da aggiungere ogni volta che viene scelto addPartitions>
-connectFile	<percorso del file salvato mediante saveConnection>

Esecuzione di partitionConfig

1. Eseguire il comando come nell'esempio seguente:

```
./sdm -action partitionConfig –freq <3D o 2D o 1D o
   1W> -days <numero di giorni da aggiungere ogni
   volta che viene scelto
   "addPartitions"> -connectFile <percorso del file
   salvato da "saveConnection" (default:
   $ESEC_HOME/sdm/sdm.connect)>
```

Nell'esempio seguente il sistema aggiungerà trenta partizioni (3 partizioni al giorno = 3 * 10).

```
./sdm -action partitionConfig –freq 3D -days 10 -
   connectFile sdm.connect
```

Nell'esempio seguente il sistema aggiungerà dieci partizioni (1 partizione al giorno = 1 * 10).

```
./sdm -action partitionConfig –freq 1D -days 10 -
   connectFile sdm.connect
```

Nell'esempio seguente il sistema aggiungerà una partizione (1 partizione per 7 giorni = 1 * 10/7).

```
./sdm -action partitionConfig -size 1W -days 10 -
   connectFile sdm.connect
```

Aggiunta di partizioni

L'azione addPartitions consente di aggiungere il numero necessario di partizioni in base alla configurazione delle partizioni indicata nelle tabelle seguenti:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Se la configurazione viene effettuata in modo da ottenere partizioni relative a 10 giorni, a ogni esecuzione di "*addPartitions*" verrà verificato se si dispone di 10 giorni di partizioni. Se si dispone di partizioni sufficienti per i 10 giorni successivi, non verrà eseguita alcuna operazione. In caso contrario, verrà aggiunto il numero di partizioni necessario per coprire i 10 giorni.

Con questa azione vengono utilizzati i flag seguenti:

-action	addPartitions
-connectFile	<percorso del file salvato da "saveConnection">

Esecuzione di addPartitions

1. Eseguire il comando come nell'esempio seguente:

   ```
   sdm -action addPartitions -connectFile <percorso del
      file salvato da "saveConnection">
   ```

   Esempio per Oracle:

   ```
   ./sdm -action addPartitions -connectFile sdm.connect
   ```

Esempio per SQL Server:

```
sdm -action addPartitions -connectFile sdm.connect
```

Abbandono di partizioni

L'azione dropPartition<1} consente di abbandonare tutte le partizioni anteriori rispetto al valore del flag keepDays dalle tabelle seguenti:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Questa azione non determina l'abbandono di partizioni non archiviate. Se si desidera eliminare partizioni non archiviate, utilizzare il flag "*forceDelete*". Se si utilizza forceDelete:

false oppure valore non specificato	vengono abbandonate solo le partizioni anteriori al valore di keepDays e le partizioni archiviate
true	vengono abbandonate tutte le partizioni anteriori al valore di keepDays incluse le partizioni non archiviate

Con questa azione vengono utilizzati i flag seguenti:

-action	dropPartitions
-keepDays	<numero di giorni di permanenza>
[-forceDelete]	<"true" o "false">
-connectFile	<percorso del file salvato da "saveConnection">

NOTA: Se si abbandona una partizione non archiviata, questa non può essere importata.

Esecuzione di dropPartitions

1. Eseguire il comando come nell'esempio seguente:

```
sdm -action dropPartitions [-forceDelete <false>] -
   keepDays <numero> -connectFile <percorso del file
   salvato da "saveConnection">
```

Negli esempi seguenti vengono abbandonate tutte le partizioni anteriori a 30 giorni e ne viene effettuata l'archiviazione. Tutte le partizioni ignorate (non rimosse) poiché non archiviate verranno elencate al termine dell'operazione.

Esempio per Oracle:

```
./sdm -action dropPartitions -keepDays 30 -connectFile
   sdm.connect


./sdm -action dropPartitions -forceDelete false -
   keepDays 30 -connectFile sdm.connect
```

Esempio per SQL Server:

```
sdm -action dropPartitions -keepDays 30 -connectFile
   sdm.connect


sdm -action dropPartitions -forceDelete false -
   keepDays 30 -connectFile sdm.connect
```

Visualizzazione di riepiloghi sulle partizioni

L'azione ViewPartitions consente di visualizzare il riepilogo delle partizioni delle tabelle supportate seguenti:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Con questo comando vengono utilizzati i flag seguenti:

-action	startGui
-tableName	<nome di una delle tabelle denominate sopra>
-connectFile	<percorso del file salvato da "saveConnection">

Per visualizzare i riepiloghi sulle partizioni

1. Eseguire il comando come nell'esempio seguente:

```
sdm -action viewPartitions -tableName <nome tabella> –
   connectFile <percorso del file salvato da
   "saveConnection">
```

Nell'esempio seguente viene visualizzato l'elenco delle partizioni della tabella EVENTS e lo stato di ognuna di esse:

- Esempio per Oracle:

```
./sdm -action viewPartitions -tableName EVENTS -
   connectFile sdm.connect
```

- Esempio per SQL Server:

```
sdm -action viewPartitions –tableName EVENTS –
   connectFile sdm.connect
```

Gestione archivi

Configurazione archivi

L'azione archiveConfig viene utilizzata per configurare l'archiviazione. Questa configurazione determina la modalità di archiviazione dei dati delle tabelle di Sentinel.

Con questa azione vengono utilizzati i flag seguenti:

-action	archiveConfig
-dirPath	<percorso di directory valido in cui scrivere i file archiviati>
-keepDays	<numero di giorni di permanenza>
-fileSize	(Solo Oracle) <dimensione massima di ogni file archiviato, espresso in KB, MB o GB>
-connectFile	<percorso del file salvato da "saveConnection">

Per Oracle, il percorso di directory dirPath deve essere specificato come parametro UTL_FILE_DIR nel file init.ora in base ai requisiti Oracle. È necessario disporre di una delle seguenti:

- UTL_FILE_DIR = *
- UTL_FILE_DIR = directory specifica in cui si desidera scrivere i file in init.ora

Esecuzione di archiveConfig

1. Eseguire il comando come nell'esempio seguente:

```
sdm -action archiveConfig  -dirPath <percorso di
   directory in cui scrivere i file archiviati> -
   keepDays <numero di giorni di permanenza> -fileSize
   <dimensione massima di ogni file archiviato,
   espressa in KB, MB o GB> -connectFile <percorso del
   file salvato da "saveConnection">
```

- Esempio per Oracle:

Nell'esempio seguente viene illustrata l'archiviazione nella directory /tmp di dati risalenti a 13 giorni prima, in porzioni superiori a 1 GB.

```
./sdm -action archiveConfig -dirPath /tmp -keepDays 13
   -fileSize 1GB -connectFile sdm.connect
```

Nell'esempio seguente viene illustrata l'archiviazione nella directory /tmp di dati risalenti a 13 giorni prima, in porzioni superiori a 40 MB.

```
./sdm -action archiveConfig -dirPath /tmp -keepDays 13
   -fileSize 40MB -connectFile sdm.connect
```

Archiviazione di dati

Eseguire l'azione archiveData dopo aver impostato la configurazione dell'archiviazione (archiveConfig). Questa configurazione consente di archiviare dati delle tabelle specificate in base alla configurazione dell'archiviazione. I dati vengono archiviati dalle tabelle seguenti:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
- SQL Server:
  - EVENTS
  - CORRELATED_EVENTS

NOTA: Le tabelle di aggregazione non vengono archiviate.

Con questo comando vengono utilizzati i flag seguenti:

-action	archiveData
-connectFile	<percorso del file salvato da "saveConnection">

Esecuzione di archiveData

1. Eseguire il comando come nell'esempio seguente:

```
sdm -action archiveData -connectFile <percorso del
   file salvato da "saveConnection">
```

- Esempio per Oracle:

Nell'esempio seguente vengono archiviati gli eventi, i valori riservati e personalizzati e gli eventi correlati delle tabelle EVENTS, EVT_RESERVED_VALUES, EVT_CUSTOM_VALUES e ASSOCIATIONS in base ai valori impostati nella configurazione dell'archiviazione (archiveConfig). Se si utilizza il valore impostato nell'esempio illustrato nella sezione relativa alla gestione degli archivi, verranno archiviati i dati anteriori a 13 giorni.

```
./sdm -action archiveData -connectFile sdm.connect
```

- Esempio per SQL Server:

Nell'esempio seguente vengono archiviati gli eventi e gli eventi correlati in base al valore impostato nella configurazione degli archivi (archiveConfig). Se si utilizza il valore impostato nell'esempio illustrato nella sezione relativa alla gestione degli archivi, verranno archiviati i dati anteriori a 13 giorni.

```
sdm -action archiveData -connectFile sdm.connect
```

Eliminazione di dati

L'azione deleteData consente di eliminare i dati anteriori ai giorni permanenza dalla tabella specificata, tra quelle seguenti:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

- SQL Server:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Questa azione non determina l'abbandono di partizioni non archiviate. Se si desidera eliminare partizioni non archiviate, è necessario specificare il flag facoltativo "*forceDelete*" impostando il valore true. Se si utilizza forceDelete:

false oppure valore non specificato	vengono abbandonate solo le partizioni anteriori al valore di keepDays e le partizioni archiviate
true	vengono abbandonate tutte le partizioni anteriori al valore di keepDays incluse le partizioni non archiviate

Con questo comando vengono utilizzati i flag seguenti:

-action	deleteData
-keepDays	<numero di giorni di permanenza>
[-forceDelete]	<true o false>
-connectFile	<percorso del file salvato da "saveConnection">

Esecuzione di deleteData

1. Eseguire il comando come nell'esempio seguente:

```
sdm -action deleteData -keepDays <numero di giorni di
   permanenza> -connectFile <percorso del file salvato
   da "saveConnection">
```

   - Esempio per Oracle:

   Nell'esempio seguente vengono abbandonate le partizioni di tutte le tabelle anteriori a 13 giorni, verificando che tutte le partizioni abbandonate siano archiviate. Al termine, viene generato un elenco delle eventuali partizioni non eliminate in quanto non archiviate.

```
./sdm -action deleteData -keepDays 13 -connectFile
   sdm.connect
```

- Esempio per SQL Server:

Nell'esempio seguente vengono abbandonate le partizioni di tutte le tabelle anteriori a 13 giorni, verificando che tutte le partizioni abbandonate siano archiviate. Al termine, verranno elencate le eventuali partizioni non eliminate in quanto non archiviate.

```
sdm -action deleteData -keepDays 13 -connectFile
   sdm.connect
```

Gestione dell'importazione

Elenco dei file da importare

L'azione filesToImport viene utilizzata per elencare i file necessari per importare i dati compresi tra le date specificate delle tabelle supportate seguenti:

- Oracle:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

Con questo comando vengono utilizzati i flag seguenti:

-action	filesToImport
-startDate	<mm/gg/aaaa hh24:mi:ss>
-endDate	<mm/gg/aaaa hh24:mi:ss>
-connectFile	<percorso del file salvato da “saveConnection”>

NOTA: per hh24 si intende il formato a 24 ore. Ad esempio 13:15:00 e 3:00:00.

Esecuzione di filesToImport

1. Eseguire il comando come nell'esempio seguente:

```
sdm -action filesToImport -startDate <mm/gg/aaaa
   hh24:mi:ss> -endDate <mm/gg/aaaa hh24:mi:ss> -
   connectFile <percorso del file salvato da
   “saveConnection”>
```

Nell'esempio seguente vengono elencati tutti i file contenenti dati compresi tra le date “09/25/2003 00:00:00” (25 settembre a mezzanotte) e “09/26/2003 00:00:00 (26 settembre a mezzanotte) archiviati precedentemente e che possono essere nuovamente importati.

- Esempio per Oracle:

```
./sdm -action filesToImport -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

- Esempio per SQL Server:

```
sdm -action filesToImport -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

Nell'esempio seguente vengono elencati tutti i file contenenti dati compresi tra le date "09/25/2003 16:00:00" (25 settembre alle 16) e "09/26/2003 18:00:00 (26 settembre alle 18) archiviati precedentemente e che possono essere nuovamente importati.

- Esempio per Oracle:

```
./sdm -action filesToImport -startDate 09/25/2003
   16:00:00 -endDate 09/26/2003 18:00:00 -connectFile
   sdm.connect
```

- Esempio per SQL Server:

```
sdm -action filesToImport -startDate 09/25/2003
   16:00:00 -endDate 09/26/2003 18:00:00 -connectFile
   sdm.connect
```

Importazione di dati

L'azione importData consente di importare i dati compresi tra le date specificate nelle tabelle supportate seguenti:

- Oracle:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

Se i dati sono già stati importanti oppure non sono disponibili dati archiviati compresi tra le date specificate, verrà restituito un messaggio.

L'applicazione importa ogni file in una tabella e genera la visualizzazione cronologica su tutte le tabelle della cronologia. Nella visualizzazione del rapporto vengono unite la tabella originale e la visualizzazione cronologica. Tutti i rapporti utilizzano tale visualizzazione e riporteranno quindi eventuali dati importati.

Con questo comando vengono utilizzati i flag seguenti:

-action	importData
-startDate	<mm/gg/aaaa hh24:mi:ss>
-endDate	<mm/gg/aaaa hh24:mi:ss>
-dirPath	<directory da cui importare i file>
-connectFile	<percorso del file salvato da "saveConnection">

NOTA: Per hh24 si intende il formato a 24 ore. Ad esempio 13:15:00 e 3:00:00.

Esecuzione di importData

1. Inserire tutti i file che si desidera importare in una directory specifica (ovvero quella specificata in dirPath - <directory da cui importare i file>).
2. Eseguire il comando come nell'esempio seguente:

```
sdm -action importData -dirPath <directory da cui
   importare i file> -startDate <mm/gg/aaaa
   hh24:mi:ss> -endDate <mm/gg/aaaa hh24:mi:ss> -
   connectFile <percorso del file salvato da
   "saveConnection">
```

Nell'esempio seguente vengono importati i file archiviati dalla directory tmp contenenti dati compresi tra le date "09/25/2003 00:00:00" (25 settembre a mezzanotte) e "09/26/2003 00:00:00 (26 settembre a mezzanotte) nelle tabelle citate sopra.

- Esempio per Oracle:

```
./sdm -action importData -dirPath /tmp -startDate
   09/25/2003 00:00:00 -endDate 09/26/2003
   00:00:00 -connectFile sdm.connect
```

- Esempio per SQL Server:

```
sdm -action importData -dirPath c:\tmp -startDate
   09/25/2003 00:00:00 -endDate 09/26/2003
   00:00:00 -connectFile sdm.connect
```

Nell'esempio seguente vengono importati i file archiviati dalla directory tmp contenenti dati compresi tra le date "09/25/2003 08:30:00" (25 settembre alle 8:30) e "09/26/2003 20:00:00 (26 settembre alle 20) nelle tabelle citate sopra.

- Esempio per Oracle:

```
./sdm -action importData -dirPath /tmp -startDate
   09/25/2003 08:00:00 -endDate 09/26/2003
   20:00:00 -connectFile sdm.connect
```

- Esempio per SQL Server:

```
sdm -action importData -dirPath c:\tmp -startDate
   09/25/2003 08:00:00 -endDate 09/26/2003
   20:00:00 -connectFile sdm.connect
```

Eliminazione di dati importati

L'azione dropImported consente di eliminare i dati compresi tra le date specificate nelle tabelle supportate seguenti:

- Oracle:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

Se non sono disponibili dati importati compresi tra le due date specificate, verrà restituito un messaggio.

Con questo comando vengono utilizzati i flag seguenti:

-action	dropImported
-startDate	<mm/gg/aaaa hh24:mi:ss>
-endDate	<mm/gg/aa hh24:mi:ss>
-connectFile	<percorso del file salvato da "saveConnection">

NOTA: Per hh24 si intende il formato a 24 ore. Ad esempio 13:15:00 e 3:00:00.

Esecuzione di dropImported

1. Eseguire il comando come nell'esempio seguente:

```
sdm -action dropImported -startDate <mm/gg/aaaa
   hh24:mi:ss> -endDate <mm/gg/aaaa hh24:mi:ss> -
   connectFile <percorso del file salvato da
   "saveConnection">
```

Nell'esempio seguente vengono eliminati i dati importati compresi tra le date specificate dalle tabelle citate sopra.

- Esempio per Oracle:

```
./sdm -action dropImported -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

- Esempio per SQL Server:

```
sdm -action dropImported -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

Gestione di spazi delle tabelle

Ai fini della gestione degli spazi delle tabelle è possibile utilizzare un'opzione della riga di comando oppure l'interfaccia utente grafica. La riga di comando consente di:

- Visualizzare l'utilizzo dello spazio del database di Sentinel

L'interfaccia utente grafica consente di:

- Visualizzare le partizioni
- Visualizzare le partizioni archiviate
- Visualizzare le partizioni importate
- Visualizzare l'utilizzo dello spazio

Visualizzazione dell'utilizzo dello spazio del database di Sentinel (riga di comando)

L'azione dbstats consente di visualizzare l'utilizzo dello spazio del database di Sentinel relativamente a tutti gli spazi delle tabelle nei filegroup di Sentinel e Oracle.

Con questo comando vengono utilizzati i flag seguenti:

-action	dbstats
-connectFile	<percorso del file salvato da "saveConnection">

Visualizzazione dell'utilizzo dello spazio del database di Sentinel (riga di comando)

1. Eseguire il comando seguente:

```
sdm -action dbStats -connectFile <percorso del file
   salvato da "saveConnection">
```

- Esempio per Oracle:

Nell'esempio seguente vengono visualizzati gli spazi delle tabelle del database di Sentinel per i quali vengono indicati, lo spazio totale, lo spazio utilizzato e lo spazio libero disponibile.

```
./sdm -action dbStats -connectFile sdm.connect
```

- Esempio per SQL Server:

Nell'esempio seguente vengono visualizzati i filegroup del database di Sentinel per i quali vengono indicati, lo spazio totale, lo spazio utilizzato e lo spazio libero disponibile.

```
sdm -action dbStats -connectFile sdm.connect
```

Aggiornamento di mappature (riga di comando)

L'azione updateMapData consente di sostituire un file dei dati di origine della mappatura con un altro. Il nuovo file di dati di origine deve avere gli stessi delimitatori, colonne chiave e colonne attivate della mappatura precedente. In caso contrario, utilizzare la funzione Modifica dell'interfaccia utente grafica di Gestione dati Sentinel.

Con questo comando vengono utilizzati i flag seguenti:

-action	updateMapData
-map	<nome mappatura>
-file	<nome file>
-backup	<true/false> (default: true)
-connectFile	<percorso del file salvato da “saveConnection”>

Il flag –backup consente di eseguire una copia di backup del file di mappatura originale nella cartella map_data. Il file di mappatura di cui si esegue il backup verrà salvato con estensione bak e una serie di numeri casuali aggiunti alla fine del nome. Ad esempio: threat10197.bak.

Aggiornamento (sostituzione) di una mappatura

1. Eseguire il comando seguente:

```
sdm -action updateMapData -map <nomemappatura> -file
   <nomefile> [-backup <true/false> (DEFAULT: true)] -
   connectFile <percorso del file salvato
   da "saveConnection">
```

Nell'esempio seguente vengono sostituite le mappature di “threat” con quelle del file di mappatura “vuln_attacks.txt”.

```
sdm -action updateMapData -map threat -file
   vuln_attacks.txt -connectFile sdm.connect
```

Poiché il flag –backup non è utilizzato, l'operazione di default determinerà la creazione di una copia di backup della mappatura originale prima dell'aggiornamento con il file di mappatura “vuln_attack.txt”.

Utilizzo dello script di gestione automatica fornito da Novell (solo per Windows)

Novell ha sviluppato un file batch di cui è possibile pianificare l'esecuzione in modo da effettuare automaticamente diverse operazioni di Gestione dati Sentinel.

NOTA: Se con il computer in uso non è possibile accedere a DAS_Binary e DAS_Query, utilizzare la riga di comando di Gestione dati Sentinel anziché l'interfaccia utente.

Questa procedura può essere applicata solo a Windows. Assicurarsi che durante l'esecuzione delle operazioni preliminari di configurazione e di configurazione effettive vengano eseguite le operazioni seguenti:

- Assicurarsi che sdm.connect venga inizializzato mediante l'interfaccia utente grafica di Gestione dati Sentinel o la riga di comando.
- Assicurarsi che la directory di archiviazione sia esistente.
- Assicurarsi che i giorni di archiveConfig e dropPartitions si equivalgano.
- Assicurarsi che i file batch vengano eseguiti correttamente dal prompt dei comandi almeno una volta prima di pianificarne l'esecuzione automatica.

NOTA: Se il task pianificato non riesce, non verrà inviata alcuna notifica ma verrà registrato in SDM_*.log

Impostazione del file Manage_data.bat per archiviare dati e aggiungere partizioni

Operazioni preliminari alla configurazione

Prima di impostare automaticamente l'archiviazione di dati e l'aggiunta di partizioni, è necessario:

- Salvare le proprietà di connessione
- Stabilire i parametri di archiviazione

NOTA: Se si salva un file di connessione in un'ubicazione o con un nome diversi da quelli di default (%ESEC_HOME%\sdm\sdm.connect), sarà necessario modificare il file manage_data.bat per aggiornare il percorso del file di connessione.

Definizione di parametri di archiviazione

È possibile eseguire questa operazione mediante la riga di comando.

L'azione archiveConfig viene utilizzata per configurare l'archiviazione. Questa configurazione determina la modalità di archiviazione dei dati delle tabelle di Sentinel.

Con questa azione vengono utilizzati i flag seguenti:

-action	archiveConfig
-dirPath	<percorso di directory valido in cui scrivere i file archiviati>
-keepDays	<numero di giorni di permanenza>
-connectFile	<percorso del file salvato da "saveConnection">

Definizione di parametri di archiviazione tramite la riga di comando

1. Creare una directory di output di archiviazione denominata SDM_archive nella directory radice (c:\SDM_archive).

   NOTA: Se si crea una directory di output o un'ubicazione diversa, sarà necessario modificare il file manage_data.bat.

2. Eseguire il comando come nell'esempio seguente:

```
sdm -action archiveConfig  -dirPath <percorso di
   directory in cui scrivere i file archiviati> -
   keepDays <numero di giorni di permanenza> -
   connectFile <percorso del file salvato da
   "saveConnection">
```

Nell'esempio seguente viene illustrata l'archiviazione nella directory c:\SDM_archive di dati risalenti a 30 giorni prima.

```
sdm -action archiveConfig –dirpath c:\SDM_archive -
   keepDays 30 -connectFile sdm.connect
```

Definizione di parametri di archiviazione tramite l'interfaccia utente grafica

1. Creare una directory di output di archiviazione denominata SDM_archive nella directory radice (c:\SDM_archive).

   NOTA: Se si crea una directory di output o un'ubicazione diversa, sarà necessario modificare il file manage_data.bat.

2. Per l'interfaccia utente grafica di gestione dati Sentinel non sono necessari parametri di archivio. L'interfaccia utente grafica supporta infatti l'archiviazione diretta dei dati senza che sia necessario definire parametri di archivio.

Eliminazione di dati (rilascio di partizioni)

L'azione deleteData consente di eliminare i dati anteriori ai giorni permanenza dalla tabella specificata, tra quelle seguenti:

- EVENTS
- CORRELATED_EVENTS
- EVT_DEST_EVT_NAME_SMRY_1
- EVT_DEST_SMRY_1
- EVT_DEST_TXNMY_SMRY_1
- EVT_PORT_SMRY_1
- EVT_SEV_SMRY_1
- EVT_SRC_SMRY_1

Questa azione non determina l'abbandono di partizioni non archiviate. Se si desidera eliminare partizioni non archiviate, è necessario specificare il flag facoltativo "*forceDelete*" impostando il valore true. Se si utilizza forceDelete:

false oppure valore non specificato	vengono abbandonate solo le partizioni anteriori al valore di keepDays e le partizioni archiviate
true	vengono abbandonate tutte le partizioni anteriori al valore di keepDays incluse le partizioni non archiviate

Con questo comando vengono utilizzati i flag seguenti:

-action	deleteData
-keepDays	<numero di giorni di permanenza>
[-forceDelete]	<true o false>
-connectFile	<percorso del file salvato da "saveConnection">

Esecuzione di deleteData

1. Eseguire il comando come nell'esempio seguente:

```
sdm -action deleteData -keepDays <numero di giorni di
   permanenza> -connectFile <percorso del file salvato
   da "saveConnection">
```

Nell'esempio seguente vengono abbandonate le partizioni delle tabelle anteriori a 30 giorni, verificando che tutte le partizioni abbandonate siano archiviate. Al termine, verranno elencate le eventuali partizioni non eliminate in quanto non archiviate.

```
sdm -action deleteData -keepDays 30 -connectFile
   sdm.connect
```

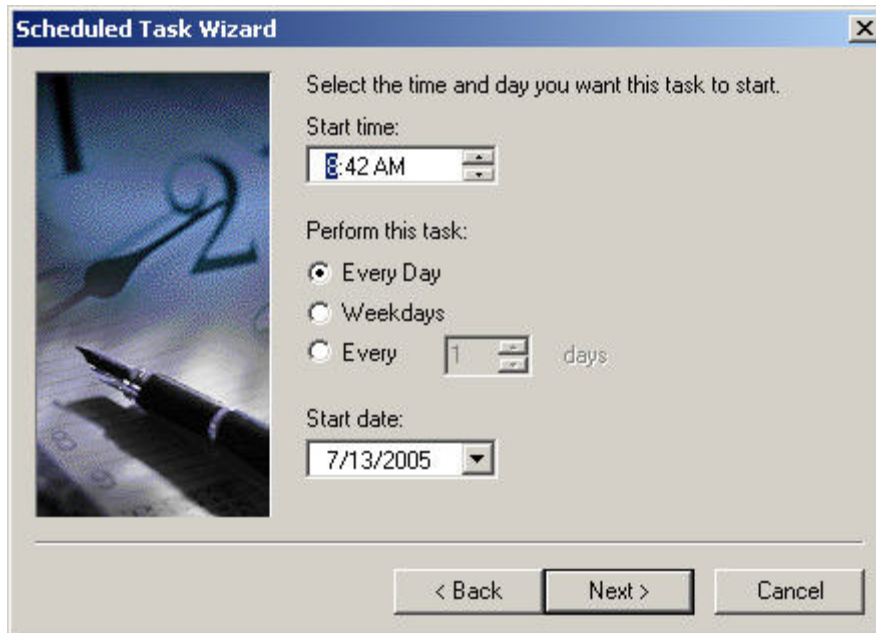
Pianificazione di Manage_data.bat per archiviare dati e aggiungere partizioni

NOTA: Il file manage_data.bat è impostato su un valore keepDays di 30, l'output di archiviazione su c:\SDM_archive e il file di connessione in %ESEC_HOME%\sdm\sdm.connect. Se i valori disponibili sono diversi, sarà necessario modificare il file manage_data.bat.

Se sono stati impostati le proprietà di connessione e i parametri di archivio, eseguire dal prompt dei comandi per garantirne il corretto funzionamento.

Per archiviare i dati e aggiungere le partizioni automaticamente

NOTA: I passaggi seguenti possono essere applicati a Windows 2000 Professional. I passaggi per Windows 2000 Server e XP possono essere diversi ma simili.

1. In Windows fare clic su Start > Impostazioni > Pannello di controllo.
2. Fare doppio clic su 'Operazioni pianificate'.
3. Fare doppio clic su *'Aggiungi operazione pianificata'*. Fare clic su *Avanti*.
4. Fare clic sul *pulsante* Sfoglia, quindi individuare il file manage_data.bat.
5. Assegnare un nome all'operazione pianificata, ad esempio SDM_Archive. Selezionare *Ogni* giorno in "*Esegui questa operazione*". Fare clic su *Avanti*.
6. Selezionare un'ora del giorno in cui eseguire questa operazione. Fare clic su *Avanti*.
7. Immettere l'ora e la data desiderate. Fare clic su *Avanti*.

8. Immettere un utente in cui verrà eseguita questa operazione. L'utente non può corrispondere al conto del sistema locale. L'operazione deve essere eseguita come utente specifico. Fare clic su *Avanti*.
9. Fare clic su *Fine* per completare l'operazione pianificata.

11 Utility

Avvio e arresto del server Sentinel e di Gestione servizi di raccolta in UNIX

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Avvio del server Sentinel in UNIX

In UNIX, con l'avvio del server Sentinel viene avviato anche Communication Server.

Avvio del server Sentinel in UNIX

1. In qualità di utente esecadm, passare alla directory $ESEC_HOME/sentinel/scripts.
2. Eseguire il comando seguente:

```
./sentinel.sh start
```

Arresto del server Sentinel in UNIX

In UNIX, con l'arresto del server Sentinel viene chiuso anche Communication Server.

Arresto del server Sentinel in UNIX

1. In qualità di utente esecadm, passare alla directory $ESEC_HOME/sentinel/scripts.
2. Eseguire il comando seguente:

```
./sentinel.sh stop
```

Avvio di Gestione servizi di raccolta in UNIX

Avvio di Gestione servizi di raccolta in UNIX

1. In qualità di utente esecadm, passare alla directory $WORKBENCH_HOME.
2. Eseguire il comando seguente:

```
./agent-manager.sh start
```

Arresto di Gestione servizi di raccolta in UNIX

Arresto di Gestione servizi di raccolta in UNIX

1. In qualità di utente esecadm, passare alla directory $WORKBENCH_HOME.
2. Eseguire il comando seguente:

```
./agent-manager.sh stop
```

Avvio e arresto del server Sentinel e di Gestione servizi di raccolta in Windows

In base alla configurazione di installazione del sistema in uso, è possibile eseguire fino a tre servizi Sentinel contemporaneamente, ovvero:

- Sentinel: servizio di sorveglianza che consente l'avvio di tutti gli altri processi del server Sentinel.
- Sentinel Communication: servizio che corrisponde a Communication Server cifrato.
- Gestione servizi di raccolta: servizio che costituisce Wizard.

In Servizi di Windows, è possibile avviare, riavviare e arrestare manualmente i suddetti servizi.

Avvio di Gestione servizi di raccolta in Windows

Avvio di Gestione servizi di raccolta in Windows

1. Fare clic su *Start* > *Impostazioni* > *Pannello di controllo*.
2. Fare doppio clic su *Strumenti di amministrazione*.
3. Fare doppio clic su *Servizi*.
4. Fare clic con il pulsante destro del mouse su Gestione servizi di *raccolta, quindi scegliere Avvia*.

Arresto di Gestione servizi di raccolta in Windows

Arresto di Gestione servizi di raccolta in Windows

1. Fare clic su *Start* > *Impostazioni* > *Pannello di controllo*.
2. Fare doppio clic su *Strumenti di amministrazione*.
3. Fare doppio clic su *Servizi*.
4. Fare clic con il pulsante destro del mouse su Gestione servizi di *raccolta, quindi scegliere Arresta*.

Avvio del server Sentinel in Windows

Avvio del server Sentinel in Windows

1. Fare clic su *Start* > *Impostazioni* > *Pannello di controllo*.
2. Fare doppio clic su *Strumenti di amministrazione*.
3. Fare doppio clic su *Servizi*.
4. Nella finestra Servizi evidenziare Sentinel.
5. Fare clic con il pulsante destro del mouse e scegliere Avvia oppure fare clic sul pulsante di avvio sulla barra degli strumenti.

Arresto del server Sentinel in Windows

Arresto del server Sentinel in Windows

1. Fare clic su *Start* > *Impostazioni* > *Pannello di controllo*.
2. Fare doppio clic su *Strumenti di amministrazione*.

3. Fare doppio clic su *Servizi*.
4. Nella finestra Servizi evidenziare *Sentinel*.
5. Fare clic con il pulsante destro del mouse e scegliere Arresta oppure fare clic sul pulsante di arresto sulla barra degli strumenti.

Avvio di Communication Server di Sentinel in Windows

Avvio di Communication Server di Sentinel in Windows

1. Fare clic su *Start* > *Impostazioni* > *Pannello di controllo.*
2. Fare doppio clic su *Strumenti di amministrazione*.
3. Fare doppio clic su *Servizi*.
4. Nella finestra Servizi evidenziare Sentinel Communication.
5. Fare clic con il pulsante destro del mouse e scegliere Avvia oppure fare clic sul pulsante di avvio sulla barra degli strumenti.

Arresto di Communication Server di Sentinel in Windows

Arresto di Communication Server di Sentinel in Windows

1. Fare clic su *Start* > *Impostazioni* > *Pannello di controllo.*
2. Fare doppio clic su *Strumenti di amministrazione*.
3. Fare doppio clic su *Servizi*.
4. Nella finestra Servizi evidenziare Sentinel Communication.
5. Fare clic con il pulsante destro del mouse e scegliere Arresta oppure fare clic sul pulsante di arresto sulla barra degli strumenti.

File di script di Sentinel

In base alla configurazione di installazione del sistema in uso, nella directory $ESEC_HOME/sentinel/scripts oppure %ESEC_HOME%\sentinel\scripts possono essere inclusi alcuni o tutti i file di script seguenti:

File di script:	**Descrizione:**
▪ remove_sonic_lock.bat	Questo script consente di rimuovere il(i) file di blocco di Communication Server.
▪ start_broker.bat ▪ start_broker.sh	Questi script consentono l'avvio di Communication Server dalla riga di comando in modalità console.
▪ stop_broker.bat ▪ stop_broker.sh	Questi script consentono l'arresto di Communication Server dalla riga di comando in modalità console.
▪ stop_container.bat ▪ stop_container.sh	Questo script consente il riavvio dei container seguenti: ▪ DAS_Aggregation ▪ DAS_RT ▪ DAS_iTRAC ▪ DAS_Binary ▪ DAS_Query

▪ sentinel.sh	Questo script consente di arrestare o avviare il server Sentinel. Vedere Avvio del server Sentinel in UNIX oppure Arresto del server Sentinel in UNIX.

Rimozione dei file di blocco di Communication Server

Se il sistema si chiude in modo non corretto, è possibile che Communication Server sia bloccato. Dopo avere rimosso i file di blocco, sarà necessario riavviare Communication Server. Questi file si trovano:

Per Windows:

```
%ESEC_HOME%\3rdparty\SonicMQ\MQ6.1\esecDomain\data\_MFSys
   tem\lock
%ESEC_HOME%\3rdparty\SonicMQ\MQ6.1\SonicMQStore\db.lck
```

Per UNIX:

```
$ESEC_HOME/3rdparty/SonicMQ/MQ6.1/esecDomain/data/_MFSyst
   em/lock
$ESEC_HOME /3rdparty/SonicMQ/MQ6.1/SonicMQStore/db.lck
```

Rimozione dei file di lock di Communication Server (Windows)

1. Passare alla directory seguente o utilizzare Esplora risorse per accedervi:

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Fare doppio clic sul file seguente (tramite Esplora Risorse) oppure eseguirlo:

   ```
   remove_sonic_lock.bat
   ```

Rimozione dei file di lock di Communication Server (UNIX)

In genere non è necessario rimuovere i file di lock in UNIX perché normalmente questi file vengono rimossi automaticamente all'avvio del server Sentinel. Per rimuovere manualmente questi file, utilizzare i comandi standard di gestione dei file UNIX (come rm).

Avvio di Communication Server in modalità console

Questi script consentono l'avvio di Communication Server dalla riga di comando in modalità console. Consentono inoltre il debug di Communication Server senza la necessità di eseguire tutto il server Sentinel. Durante il normale svolgimento delle operazioni, questi script non devono essere utilizzati (seguire le istruzioni fornite nelle sezioni Avvio del server Sentinel in UNIX o Avvio del server Sentinel in Windows).

Avvio di Communication Server (Windows)

NOTA: Se avviato in Windows, questo script non risulta nella finestra Servizi e verrà eseguito solo se la finestra del prompt dei comandi rimane aperta.

1. Passare alla directory seguente o utilizzare Esplora risorse per accedervi:

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Fare doppio clic sul file seguente (tramite Esplora Risorse) oppure eseguirlo:

```
start_broker.bat
```

Avvio di Communication Server (UNIX)

1. Eseguire il login come utente esecadm.
2. Passare alla directory:

```
$ESEC_HOME/sentinel/scripts
```

3. Immettere:

```
./start_broker.sh
```

Arresto di Communication Server in modalità console

Questi script consentono l'arresto di Communication Server dalla riga di comando in modalità console. Consentono inoltre il debug di Communication Server senza la necessità di arrestare completamente il server Sentinel. Durante il normale svolgimento delle operazioni, questi script non devono essere utilizzati (seguire le istruzioni fornite nelle sezioni Arresto del server Sentinel in UNIX o Arresto del server Sentinel in Windows).

Arresto di Communication Server (Windows)

1. Passare alla directory seguente o utilizzare Esplora risorse per accedervi:

```
%ESEC_HOME%\sentinel\scripts
```

2. Fare doppio clic sul file seguente (tramite Esplora Risorse) oppure eseguirlo:

```
stop_broker.bat
```

Arresto di Communication Server (UNIX)

1. Eseguire il login come utente esecadm.
2. Passare alla directory:

```
$ESEC_HOME/sentinel/scripts
```

3. Immettere:

```
./stop_broker.sh
```

Riavvio dei container di Sentinel

Questo script consente il riavvio dei container elencati sotto. Lo script consente di inviare un messaggio al servizio specificato per determinarne la chiusura. Il servizio di sorveglianza di Sentinel poi riavvia il servizio.

Il modo migliore di arrestare, avviare o riavviare i servizi dei container consiste nell'utilizzo dell'opzione Visualizzazioni server disponibile nella scheda Amministratore di Sentinel Control Center.

Nome	Descrizione
▪ DAS_Aggregation	(das_aggregation.xml) è utilizzato per eseguire e configurare il servizio di aggregazione.
▪ DAS_RT	(das_rt.xml) è utilizzato per eseguire e configurare il servizio di

visualizzazioni in tempo reale.

- DAS_iTRAC (das_itrac.xml) è utilizzato per configurare il servizio iTRAC.
- DAS_Binary (das_binary.xml) è utilizzato per gli eventi e le operazioni di inserimento di eventi correlati.
- DAS_Query (das_query.xml) è utilizzato per tutte le altre operazioni di database.

Riavvio di un container di Sentinel (Windows)

1. Passare alla directory:

```
%ESEC_HOME%\sentinel\scripts
```

2. Immettere:

```
stop_container.bat <computer host> <nome container>
```

Ad esempio:

```
stop_container.bat localhost DAS_RT
```

Riavvio di un container di Sentinel (UNIX)

1. Eseguire il login come utente esecadm.
2. Passare alla directory:

```
$ESEC_HOME/sentinel/scripts
```

3. Immettere:

```
./stop_container <computer host> <nome container>
```

Ad esempio:

```
./stop_container localhost DAS_RT
```

Informazioni sulle versioni

Informazioni sulla versione del server Sentinel

Il server Sentinel include un’opzione nella riga di comando che consente di visualizzare informazioni sulla versione dei processi seguenti:

- sorveglianza
- rulelg_checker
- correlation_engine
- data_synchronizer
- query_manager
- DAS

Ottenere informazioni sulla versione di Sentinel (UNIX)

1. Passare alla directory:

```
$ESEC_HOME/sentinel/bin
```

2. Immettere:

```
./<processo> -version
```

Ad esempio:

```
./correlation_engine –version
```

Ottenere informazioni sulla versione di Sentinel (Windows)

1. Passare alla directory:

```
%ESEC_HOME%\sentinel\bin
```

2. Immettere:

```
./<processo> -version
```

Ad esempio:

```
./correlation_engine –version
```

Informazioni sulla versione dei file .dll e .exe di Sentinel

Ottenere informazioni sulla versione dei file.dll e .exe di Sentinel

1. Passare alla directory %ESEC_HOME%.
2. All'interno delle varie sottodirectory, fare clic con il pulsante destro del mouse su un file .dll o .exe e selezionare Proprietà.
3. Fare clic sulla scheda Versione.
4. Nel riquadro Nome elemento selezionare Versione del prodotto. Il numero di versione del file verrà visualizzato nel riquadro Valore.

Informazioni sulla versione del file .jar di Sentinel

Ottenere informazioni sulla versione del file .jar di Sentinel

1. Nel server Sentinel, eseguire il login come utente:

   Per UNIX:

```
esecadm
```

   Per Windows, eseguire il login come utente con diritti per il server Sentinel.

2. Passare alla directory:

   Per UNIX:

```
$ESEC_HOME/utilities
```

   Per Windows:

```
%ESEC_HOME%\utilities
```

3. Sulla riga di comando, digitare:

   Per UNIX:

```
./versionreader.sh <percorso/nome file jar>
```

   Per Windows

```
versionreader <percorso/nome file jar>
```

Configurazione della posta elettronica di Sentinel

Le impostazioni di configurazione della posta elettronica di Sentinel sono memorizzate nel file execution.properties durante l'installazione. È possibile modificare questo file dopo l'installazione. Il file si trova nel computer in cui è installato DAS, nella directory:

Per Windows:

```
%ESEC_HOME%\sentinel\config
```

Per UNIX:

```
$ESEC_HOME/sentinel/config
```

Esistono due script (mailconfig.sh e mailconfigtest.sh per UNIX e mailconfig.bat e mailconfigtest.bat per Windows) che consentono di modificare e verificare le impostazioni della posta elettronica all'interno del file execution.properties. Lo script mailconfig.* modifica le impostazioni delle posta elettronica mentre lo script mailconfigtest.* le verifica. Le aree evidenziate in grassetto corrispondono alle impostazioni della posta elettronica che possono essere modificate.

Nel file execution.properties sono incluse le proprietà seguenti:

mail.authentication.user=<domain\\user>	
attesa tentativi eventi correlati=5000	
mail.smtp.host=<SMTP_HOST>	L'host SMTP che sarà utilizzato per inviare i messaggi di posta elettronica.
mail.events.max=1000	Numero massimo di eventi che possono essere inviati in un messaggio di posta elettronica che viene automaticamente attivato dal motore di correlazione. Lo scopo è di limitare le dimensioni dei messaggi di posta elettronica per gli eventi correlati che hanno un numero elevato di eventi trigger.
numero tentativi eventi correlati=10	
mail.address.from=<SMTP_FROM_ADDR>	L'indirizzo e-mail visualizzato nel campo Da del messaggio inviato da DAS.
mail.authentication.password=<password>	Password per mail.authentication.user.

Negli script mailconfig.sh e mailconfig.bat sono utilizzati gli argomenti seguenti:

-host	Nome host SMTP o indirizzo IP
-from	Campo Da del messaggio e-mail
-user	L'utente di autenticazione della posta
-password	Password per l'utente di autenticazione della posta

NOTA: Non immettere la password dopo l'argomento –password. Dopo aver immesso il comando verrà richiesto di specificare una nuova password. L'output della console sarà mascherato da asterischi (*).

Nei file mailconfigtest.sh e mailconfig.bat sono utilizzati gli argomenti seguenti:

-to Indirizzo e-mail di destinazione

Per impostare le proprietà della posta elettronica nel file execution.properties

1. Nel computer in cui è installato DAS, passare alla directory seguente:

   Per UNIX:

   ```
   $ESEC_HOME/sentinel/config
   ```

   Per Windows

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Eseguire il comando mailconfig come indicato di seguito:

   Per UNIX:

   ```
   ./mailconfig.sh -host <server SMTP> -from <indirizzo
     e-mail di origine> -user <utente autenticazione
     posta> –password
   ```

   Per Windows:

   ```
   mailconfig.bat -host <server SMTP> -from <indirizzo e-
     mail di origine> -user <utente autenticazione
     posta> –password
   ```

   Esempio per UNIX:

   ```
   ./mailconfig.sh -host 10.0.1.14 -from
     my_name@domain.com -user my_user_name –password
   ```

   Esempio per Windows:

   ```
   ./mailconfig.sh -host 10.0.1.14 -from
     my_name@domain.com -user my_user_name –password
   ```

   Dopo aver immesso questo comando verrà richiesto di specificare una nuova password.

   ```
   Immettere la password:*********
   ```

   ```
   Confermare la password:*********
   ```

   NOTA: Quando si utilizza l'opzione relativa alla password, deve trattarsi dell'ultimo argomento.

Per verificare le impostazioni della posta elettronica nel file execution.properties

1. Nel computer in cui è installato DAS, passare alla directory seguente:

   Per UNIX:

   ```
   $ESEC_HOME/sentinel/config
   ```

   Per Windows

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Eseguire il comando mailconfigtest come indicato di seguito:

   Per UNIX:

```
./mailconfigtest.sh -to <indirizzo e-mail di
   destinazione>
```

Per Windows:

```
mailconfigtest.bat -to <indirizzo e-mail di
   destinazione>
```

Se l'invio del messaggio e-mail è riuscito correttamente, il messaggio sarà ricevuto all'indirizzo di destinazione e verrà visualizzato il messaggio seguente sullo schermo dell'utente.

```
Messaggio e-mail inviato!
```

Controllare la casella postale e-mail per confermare la ricezione del messaggio. La riga dell'oggetto e il contenuto dovrebbero essere:

```
Oggetto: Testing Sentinel mail property

This is a test for Sentinel mail property set up. If
   you see this message, your Sentinel mail property
   has been configured correctly to send emails
```

Aggiornamento del codice di licenza

Se il codice di licenza di Sentinel è scaduto e Novell ne ha fornito uno nuovo, eseguire il programma dei codici software per aggiornare la licenza.

Aggiornamento del codice di licenza (UNIX)

1. Eseguire il login come utente esecadm.
2. Aprire $ESEC_HOME/utilities.
3. Immettere il comando seguente:

   ```
   ./softwarekey
   ```

4. Immettere il numero 1 per impostare la chiave primaria. Premere Invio.

Aggiornamento del codice di licenza (Windows)

1. Eseguire il login come utente con diritti di amministrazione.
2. Aprire %ESEC_HOME%\utilities.
3. Immettere il comando seguente:

   ```
   softwarekey.exe
   ```

4. Immettere il numero 1 per impostare la chiave primaria. Premere Invio.

12 Avvio rapido

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo sono descritte le procedure di riferimento rapido per i responsabili di:

- Analisi della sicurezza
- Analisi dei rapporti
- Amministrazione

Sono trattati gli argomenti seguenti:

- Active Views™
- Rilevamento degli exploit
- Dati delle risorse
- Interrogazione eventi
- Rapporti di analisi tramite Crystal Reports
- Correlazione di base

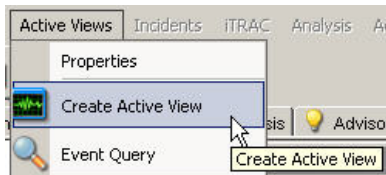
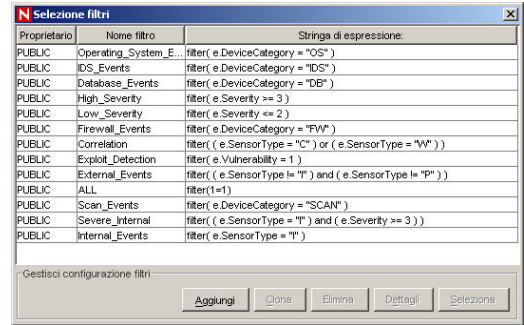
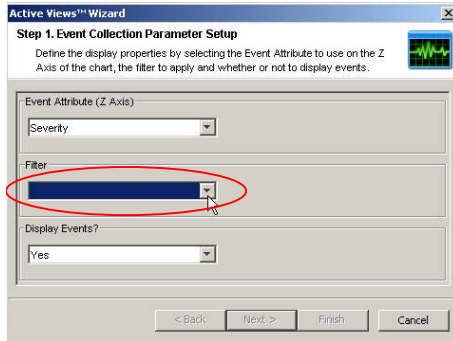
Analisi della sicurezza

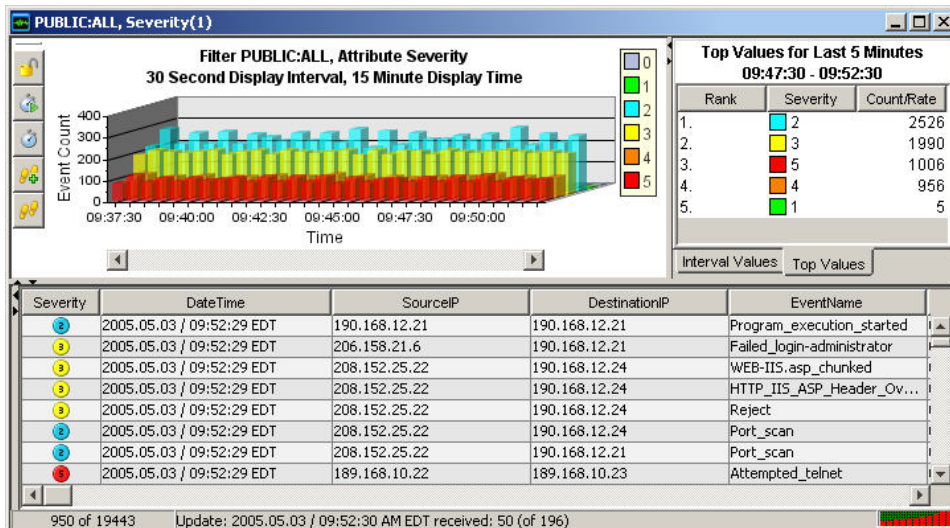
NOTA: L'amministratore responsabile della sicurezza del sistema, o l'utente, deve avere creato i filtri necessari e configurato i Servizi di raccolta appropriati per il sistema.

Scheda Active Views

Nella scheda Active Views, è possibile monitorare gli eventi che si verificano tramite interrogazioni. Il monitoraggio degli eventi può essere eseguito in una tabella oppure attraverso una rappresentazione grafica 3-D.

Per avviare un evento in tempo reale

1. Fare clic su *Active Views, scegliere Crea visualizzazione* Active Views, quindi fare clic sulla freccia giù Filtro, selezionare un filtro e fare clic sul pulsante *Seleziona*.

2. Fare clic su *Fine*. Se è attiva una connessione in rete, può essere visualizzata una schermata simile a quella illustrata sotto:

NOTA: Per visualizzare un grafico 3-D senza eventi in tempo reale, fare clic sulla freccia giù Visualizzare gli eventi? e selezionare No.

Rilevamento degli exploit

Per visualizzare gli eventi che indicano un possibile exploit, è necessario disporre degli elementi seguenti:

- feed di dati di Advisor
- rilevamento delle intrusioni
- scansione delle vulnerabilità

All'interno di un evento, se il valore nel campo Vulnerabilità (*vul*) è pari a 1, significa che la risorsa o il dispositivo di destinazione è sfruttato. Se invece il valore nel campo Vulnerabilità è pari a 0, significa che la risorsa o il dispositivo di destinazione non è sfruttato. Se il campo Vulnerabilità è vuoto, la funzionalità di rilevamento degli exploit di Sentinel non è attiva.

Per visualizzare gli eventi che indicano un possibile sfruttamento, è necessario creare una visualizzazione Active Views e applicare un filtro in cui il valore di vulnerabilità sia pari a 1.

Se si dispone di Nmap e si utilizza il Servizio di raccolta Nmap, è possibile visualizzare le informazioni relative alla risorsa sfruttata o a qualsiasi altra risorsa.

Per ulteriori informazioni sul funzionamento del sistema di rilevamento degli exploit e sui sistemi di rilevamento delle intrusioni e di scansione delle vulnerabilità supportati, consultare il *Capitolo 1: Introduzione oppure il Capitolo 10: Gestione dati Sentinel*.

Dati delle risorse

Per visualizzare le informazioni sulle risorse degli eventi, fare clic con il pulsante destro del mouse su uno o più eventi, quindi scegliere Analisi e fare clic su Dati risorsa. Verrà visualizzata una finestra simile a quella riportata qui sotto.

Asset Report

desk.acmeinc.net

Hardware

MAC Address	A0:12:56:78:90:00		
Name	Build Machine	**Value**	500
Type	Server	**Criticality**	High
Vendor	Dell	**Sensitivity**	Low
Product	Precision	**Environment**	Production
Version	360	**Location**	Internal

Network

IP	Hostname
199.16.2.23	desk.acmeinc.net

Software

Name	Type	Vendor	Product	Version
ClearCase	APPLICATION	IBM	ClearCase	5.0
C++	APPLICATION	Microsoft	Visual C++	6.0

Contacts

Order	Name	Role	Email	Phone Number
1	Erickson, Stein	USER	serickson@acmedomain.net	(703) 555-8865
2	IT	Administrator	LAN_FOLKS@acemedomain.net	(703) 555-9876

Location

Room	server room
Rack	#17
Address	HQ Agent 86 Security Circle Suite 86 Washington DC 12345 USA

Interrogazione eventi

Scenario di esempio: durante il monitoraggio, sono visualizzati numerosi tentativi di Telnet dall'IP di origine 189.168.10.22. I tentativi Telnet possono essere un attacco. Potenzialmente Telnet consente a un aggressore di connettersi in modalità remota a un computer remoto e utilizzarlo come se fosse collegato localmente. Ciò può determinare modifiche di configurazione non autorizzate, l'installazione di programmi, la diffusione di virus e così via.

È possibile utilizzare il comando Interrogazione eventi per stabilire con quale frequenza l'ipotetico aggressore abbia tentato di collegarsi al sistema tramite Telnet. A tal fine, è possibile impostare un filtro per interrogare quel particolare aggressore. Si hanno a disposizione le informazioni seguenti:

- IP di origine: 189.168.10.22
- IP di destinazione: 189.168.10.23
- Gravità: 5
- Nome evento: Attempted_telnet
- Tipo di sensore: H (Rilevamento delle intrusioni host)

Per eseguire l'interrogazione di un evento

1. Fare clic sul pulsante Interrogazione eventi (icona con la lente d'ingrandimento), quindi fare clic sulla freccia giù Filtro.
2. Fare clic su Aggiungi, immettere un nome per il filtro di "telnet SIP 89_168_10_22". Nel campo sotto il filtro, digitare:
   - SourceIP (IP di origine) = 189.168.10.22
   - EventName (nome evento) = Attempted_telnet
   - Corrispondenza se, select (and)
   - Severity (Gravità) = 5
   - SensorType (tipo sensore) = H
   - DestinationIP (IP di destinazione) = 189.168.10.23
3. Fare clic su Salva. Evidenziare un filtro e fare clic su *Seleziona*.
4. Specificare l'arco temporale desiderato, quindi fare clic sul pulsante Cerca (icona con la lente d'ingrandimento). Verranno visualizzati i risultati dell'interrogazione.

Severity	DateTime	SourceIP	DestinationIP	EventName
5	2005.05.03 / 09:25:24 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:22 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:20 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:18 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:16 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:14 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:12 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:10 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:08 EDT	189.168.10.22	189.168.10.23	Attempted_telnet
5	2005.05.03 / 09:25:06 EDT	189.168.10.22	189.168.10.23	Attempted_telnet

Per determinare con quale frequenza l'utente tenti di collegarsi tramite Telnet, rimuovere DestinationIP (IP di destinazione), SensorType (Tipo sensore) e Gravità dal filtro oppure creare un filtro nuovo. Nei risultati saranno visualizzati tutti gli IP di destinazione a cui l'utente tenta di connettersi tramite Telnet.

Se uno o più eventi sono correlati (SensorType = C o W), è possibile fare clic con il pulsante destro del mouse sul comando Visualizza eventi trigger per individuare quali eventi abbiano attivato l'evento correlato.

Un numero eccessivo di eventi FTP può rappresentare un altro evento di rilievo. Può trattarsi di una connessione remota che consente il trasferimento, la copia e l'eliminazione di file.

Di seguito è proposto un breve elenco di attacchi a cui è consigliabile prestare attenzione. Esistono molti tipi di attacchi. Per reperire ulteriori informazioni sugli attacchi di rete o host, sono disponibili numerose risorse (ovvero, libri e Internet) che illustrano in modo dettagliato i diversi tipi di attacchi.

- SYN flood
- ICMP flood e UDP flood
- Sniffing di pacchetti
- Denial of Service
- Attacchi "smurf" e "fraggle"
- Attacco con dizionario

Analisi dei rapporti

NOTA: L'amministratore della sicurezza del sistema deve avere configurato il server Web Crystal Enterprise e pubblicato l'elenco dei rapporti disponibili.

Scheda Analisi

La scheda Analisi consente di eseguire rapporti cronologici. I rapporti cronologici e sulle vulnerabilità sono pubblicati su un server Web Crystal ed eseguiti direttamente sul database di Sentinel. Tali rapporti consentono di tenere traccia delle attività e analizzarle per un lungo periodo di tempo, ad esempio una settimana o un mese. Possono inoltre essere utilizzati come ottimo metodo di presentazione dei rapporti ai supervisori. Se è installato il server Web per la creazione di rapporti, individuare nella barra di navigazione i rapporti disponibili.

NOTA: L'esempio proposto di seguito riguarda Crystal 9. Le procedure di Crystal 11 sono identiche ma con nomi di rapporti differenti.

Se, ad esempio, si è responsabili della creazione di rapporti da presentare agli alti dirigenti della propria azienda, è probabile che si utilizzi SourceDestinationReports. Si tratta delle 10 principali coppie di indirizzi IP di origine-destinazione relativi a nomi host, porte, IP e utenti. Per eseguire questo rapporto, utilizzare la procedura seguente:

Esecuzione di Crystal Reports

1. Espandere ed evidenziare le 10 principali coppie di indirizzi IP di origine-destinazione e fare clic sul pulsante Crea rapporto (lente di ingrandimento).
2. Digitare esecrpt (per autenticazione SQL e Oracle) come nome utente oppure il nome utente di autenticazione di Windows e immettere la password.
3. In Report Type (Tipo di rapporto), selezionare Weekly Report (Settimanale), per fare riferimento a un intervallo di date specifico, selezionare Specific Date Range (Intervallo di date specifico).

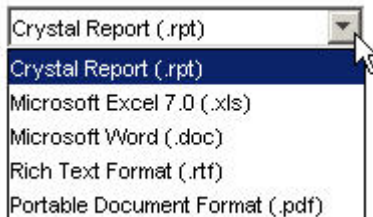
NOTA: È possibile che altri rapporti abbiano ulteriori parametri come il nome della risorsa e il livello di gravità.

4. Fare clic su View Report (Visualizza rapporto).

Top 10 Source to Destination IP Pairs: Weekly

Report Description: This report summarizes the Top 10 Pairs of Source IP Addresses and Destination IP Addresses for the **last full week** from all sensors (i.e., event sources) monitored by e-Security Agents.

Source IP	Destination IP	Number of Occurences
206.158.21.6	189.168.10.22	4,174
206.158.23.8	192.168.11.23	2,880
208.152.25.22	190.168.12.21	1,154
10.0.20.5	192.168.0.1	1,152
10.0.20.7	192.168.0.4	579
10.0.20.4	192.168.0.7	577
207.25.71.204	207.25.71.204	576
199.168.10.25	199.168.11.22	576
199.168.10.22	199.168.10.22	576
190.168.12.21	190.168.12.21	576

5. È possibile esportare il file in un documento di Word, PDF, rtf, Excel o come Crystal Report facendo clic sul pulsante Esporta (icona con la busta).

Interrogazione eventi

Analogamente alla procedura di analisi della sicurezza, se nei rapporti ci sono uno o più eventi di rilievo, è possibile effettuarne l'interrogazione utilizzando la scheda Analisi. Per eseguire un'interrogazione, evidenziare Interrogazioni cronologiche, scegliere Interrogazioni eventi cronologia e fare clic sul pulsante Crea rapporto (lente d'ingrandimento). Per ulteriori informazioni, consultare la sezione Analisi della sicurezza: scenario di esempio di interrogazione degli eventi.

Amministrazione

Correlazione base

La correlazione è il processo di analisi degli eventi di sicurezza per identificare le potenziali relazioni tra due o più eventi. Tramite la correlazione, è possibile eseguire una rapida associazione degli attacchi di priorità sulla base degli elementi comuni dei dati di eventi.

In riferimento allo scenario Telnet descritto nella sezione Analisi della sicurezza: scenario di esempio di interrogazione degli eventi, è possibile creare una regola di correlazione di base che attivi un evento correlato in seguito a quattro tentativi Telnet eseguiti in un arco di tempo di 10 secondi.

Per creare una regola di correlazione

1. Aprire la scheda Amministratore ed evidenziare Regole di correlazione nella barra di spostamento.
2. Creare una nuova cartella per l'archiviazione della regola. Tale operazione viene eseguita tramite l'utilizzo di un'opzione attivabile con il pulsante destro del mouse.
3. Evidenziare Correlazione base, immettere un nome e fare clic su Avanti. Nel riquadro successivo, fare clic sulla freccia giù e selezionare Gestione filtri. Fare clic sulla freccia giù Filtro selezionato e nel riquadro Selezione filtri fare clic su Aggiungi.
4. Digitare quanto segue:
   - Nome: telnet_attempt_189_168_10_22
   - Nome filtro: telnet attempt 189_168_10_22
   - SourceIP (IP di origine) = 189.168.10.22
   - EventName (nome evento) = Attempted_telnet
   - select *And*
   - Severity (Gravità) = 5
   - SensorType (tipo sensore) = H
   - DestinationIP (IP di destinazione) = 189.168.10.23

5. Fare clic su Salva. Evidenziare un filtro e fare clic su Seleziona.
6. Fare clic su Avanti, immettere il valore 4 se la condizione viene soddisfatta e specificare 10 secondi nel riquadro Criteri raggruppamento e soglia. Fare clic su Avanti.
7. Nel riquadro Azioni ed evento correlato, modificare il livello di gravità sul valore 2 (fare clic sulla freccia giù). Fare clic su Fine.
8. Per distribuire questa regola, evidenziare Gestione motore di correlazione nel riquadro di navigazione, evidenziare un motore di correlazione e fare clic con il pulsante destro del mouse su *Distribuisci regole*. Nel riquadro Distribuisci regole, individuare la regola creata e contrassegnarla con un segno di spunta. Fare clic su *OK*. Assicurarsi che il motore di correlazione e la regola di correlazione desiderati siano abilitati, ovvero contrassegnati con un segno di spunta verde. Tale operazione viene eseguita utilizzando il pulsante destro del mouse.
9. Per verificare la presenza di eventi correlati, esistono diversi metodi. È possibile:
   - Creare una finestra di eventi Active Views utilizzando il filtro di correlazione creato.
   - Creare una finestra di eventi Active Views utilizzando il filtro di correlazione fornito.
   - Creare una finestra di eventi Active Views utilizzando il filtro Tutti fornito, eseguire un'istantanea e ordinare gli eventi in base a SensorType (tipo sensore), quindi visualizzarli tutti impostando SensorType (tipo sensore) sul valore C.
   - Eseguire un'interrogazione rapida utilizzando il filtro creato o il filtro di correlazione.

   Fare clic con il pulsante destro del mouse sull'evento correlato, quindi selezionare Visualizza eventi trigger per scoprire quanti eventi Telnet (potrebbero essere più di 4) abbiano attivato la regola di correlazione.

Eventi di sistema di Sentinel 5

NOTA: Il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Nelle tabelle descrittive seguenti, i termini in corsivo racchiusi tra <…> sono sostituiti dai valori appropriati nei messaggi reali.

Eventi di autenticazione

Autenticazione non riuscita

Se si verifica un errore durante l'autenticazione di un utente, viene generato l'evento seguente.

Tag	Valore
Severity	4
Event Name	AuthenticationFailed
Resource	UserAuthentication
SubResource	Authenticate
Message	Errore di autenticazione dell'utente <*nome*> con il nome OS <*domUtente*> da <*IP*>

Evento utente non disponibile

Quando un utente tenta di accedere all'applicazione e viene autenticato correttamente ma non è un utente Sentinel, viene generato l'evento seguente.

Tag	Valore
Severity	4
Event Name	NoSuchUser
Resource	UserAuthentication
SubResource	Authenticate
Message	Non è stato trovato alcun utente con il nome <*nome*>

Oggetti utente duplicati

Se è presente un secondo oggetto utente attivo imprevisto, viene generato l'evento seguente. Questo è un errore interno.

Tag	Valore
Severity	4
Event Name	TooManyActiveUsers
Resource	UserAuthentication
SubResource	Authenticate
Message	Errore nella tabella utente: sono stati trovati più utenti con il nome <*nome*>

Conto bloccato

Quando si tenta di eseguire il login da un conto utente bloccato, viene generato l'evento seguente.

Tag	Valore
Severity	4
Event Name	LockedUser
Resource	UserAuthentication
SubResource	Autenticazione
Message	Tentativo di eseguire il login utilizzando il conto <*acct*> bloccato

Sessioni utente

Utente disconnesso

Quando un utente effettua il logout, viene generato l'evento interno seguente.

Tag	Valore
Severity	1
Event Name	UserLoggedOut
Resource	UserSessionManager
SubResource	User
Message	Chiusura della sessione per <*utente*> nome OS <*nomeOS*> da <*IP*> collegato da <*data*>; <*num*> utenti attualmente attivi

Utente connesso

Quando un utente effettua il login, viene generato l’evento interno seguente.

Tag	Valore
Severity	1
Event Name	UserLoggedIn
Resource	UserSessionManager
SubResource	User
Message	Utente <utente> con nome OS <nomeOS>, <IP> connesso; <num> utenti attualmente attivi

Utente rilevato

Se il server viene riavviato, le informazioni della sessione vanno perse. La sessione viene ricostruita quando si ricevono messaggi dagli utenti attivi. Quando il server rileva un utente connesso, viene generato l'evento interno seguente.

Tag	Valore
Severity	1
Event Name	UserLoggedIn
Resource	UserSessionManager
SubResource	User

Tag	Valore
Message	È stato rilevato che l'utente attivo <utente> con nome OS <nomeOS>, <IP> è connesso; <num> utenti attualmente attivi

Evento

Errore durante lo spostamento di un file completato

Un volta completato, il file di evento viene spostato nella directory di output. Se si verifica un errore durante tale operazione, viene generato l'evento interno seguente.

Tag	Valore
Severity	3
Event Name	MoveArchiveFileFailed
Resource	<Nome DAS>
SubResource	ArchiveFile
Message	Errore durante lo spostamento del file di archivio completato <nomef> nella <dir>

Errore durante l'inserimento di eventi

Se si verifica un errore durante l'inserimento di eventi nel database, viene generato l'evento interno seguente.

Tag	Valore
Severity	5
Event Name	InsertEventsFailed
Resource	EventSubSystem
SubResource	Events
Message	Errore durante l'inserimento di eventi nel database; gli eventi si possono perdere definitivamente. Verificare il database e i log del server di backend <Exception>

Errore durante l'apertura di un file di archivio

Se si verifica un errore durante l'apertura di un file di archivio per la memorizzazione degli eventi di aggregazione, verrà generato l'evento interno seguente.

Tag	Valore
Severity	3
Event Name	OpenArchiveFileFailed
Resource	<Nome DAS>
SubResource	ArchiveFile
Message	Errore durante l'apertura del file di archivio <nome> in <dir>

Errore di scrittura nel file di archivio

Se si verifica un errore durante l'apertura di un file di archivio per la memorizzazione degli eventi di aggregazione, verrà generato l'evento interno seguente.

Tag	Valore
Severity	3
Event Name	WriteArchiveFileFailed
Resource	<Nome DAS>
SubResource	ArchiveFile
Message	Errore di scrittura degli eventi appena ricevuti nel file di archivio per l'aggregazione <nomef>

Scrittura nella partizione di overflow (P_MAX)

All'incirca ogni cinque minuti, viene inviato un evento che comunica all'utente quando gli eventi vengono scritti nella partizione di overflow (P_MAX). Quando ciò si verifica, l'amministratore deve utilizzare Gestione dati Sentinel e aggiungere altre partizioni perché altrimenti le prestazioni possono essere compromesse.

Tag	Valore
Severity	5
Event Name	InsertIntoOverflowPartition
Resource	EventSubSystem
SubResource	Events
Message	Errore: scrittura nelle partizioni di overflow (P_MAX), aggiungere altre partizioni

Inserimento di eventi bloccato

Se il servizio DAS scrive nella partizione di overflow e l'utente tenta di aggiungere altre partizioni, Gestione dati Sentinel invierà una richiesta a DAS per interrompere temporaneamente l'inserimento di eventi nel database. Quando ciò accade, DAS invia eventi interni a ogni tentativo di inserimento di eventi nel database.

Tag	Valore
Severity	4
Event Name	EventInsertionIsBlocked
Resource	EventSubSystem
SubResource	Events
Message	Inserimento di eventi bloccato, attesa <num> secondi

Ripristino inserimento di eventi

Quando l'inserimento degli eventi riprende dopo il blocco, viene inviato l'evento seguente:

Tag	Valore
Severity	2
Event Name	EventInsertionResumed
Resource	EventSubSystem
SubResource	Events
Message	L'inserimento degli eventi riprende dopo il blocco

Lo spazio del database ha raggiunto il limite di tempo specificato

Quando l'inserimento degli eventi riprende dopo il blocco, viene inviato l'evento seguente.

Tag	Valore
Severity	0
Event Name	DbSpaceReachedTimeThrshld
Resource	Database
SubResource	Database
Message	Lo spazio delle tabelle <stringa> dispone ancora di <num> MB e <num> byte al secondo e si esaurirà entro il limite di tempo specificato di <num> secondi

Lo spazio del database ha raggiunto il limite percentuale specificato

Quando l'inserimento degli eventi riprende dopo il blocco, viene inviato l'evento seguente.

Tag	Valore
Severity	0
Event Name	DbSpaceReachedPercentThrshld
Resource	Database
SubResource	Database
Message	Lo spazio delle tabelle <stringa> ha una dimensione attuale di <num> MB, che può arrivare al massimo a <num> MB, e ha raggiunto il limite percentuale di <num> %

Spazio del database molto ridotto

Quando l'inserimento degli eventi riprende dopo il blocco, viene inviato l'evento seguente.

Tag	Valore
Severity	5
Event Name	DbSpaceVeryLow
Resource	Database
SubResource	Database
Message	Lo spazio delle tabelle <stringa> ha una dimensione attuale di <num> MB e ha raggiunto il limite fisico di <num> MB

Aggregazione

Errore durante l'inserimento di dati di riepilogo nel database

Se si verifica un errore durante la scrittura dei dati di aggregazione nel database, viene generato l'evento interno seguente.

Tag	Valore
Severity	4
Event Name	SummaryUpdateFailure
Resource	Aggregation
SubResource	Summary
Message	Errore durante il salvataggio di dati di riepilogo nel database per il riepilogo <nomeRiepilogo>

Servizio di mappatura

Errore di inizializzazione di mappe con ID

Questo evento interno viene generato dal lato client del servizio di mappatura, ovvero il servizio che fa parte di Gestione servizi di raccolta. Questo errore viene generato quando Gestione servizi di raccolta tenta di recuperare una mappa inesistente. Ciò può verificarsi quando si creano e si eliminano mappe.

Tag	Valore
Severity	4
Event Name	ErrorNoSuchMap
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Errore di inizializzazione di mappe con ID <ID>: mappa inesistente

Aggiornamento della mappa dalla cache

Questo evento interno viene generato dal lato client del servizio di mappatura, ovvero il servizio che fa parte di Gestione servizi di raccolta. Quando in Gestione servizi di raccolta viene ricevuta l'istruzione di aggiornamento della mappatura in seguito a modifiche sopraggiunte o al cambiamento della relativa definizione, viene generato un evento interno. Ciò significa che la cache viene aggiornata e la mappa viene aggiornata dalla cache.

Tag	Valore
Severity	1
Event Name	LoadingMapFromCache
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Caricamento della mappa<nomeMappa> (ID <id>) dalla cache v<versione>

Aggiornamento della mappa dal server

Questo evento interno viene generato dal lato client del servizio di mappatura, ovvero il servizio che fa parte di Gestione servizi di raccolta. Quando in Gestione servizi di raccolta viene ricevuta l'istruzione di aggiornamento della mappatura in seguito a modifiche sopraggiunte o al cambiamento della relativa definizione, viene generato un evento interno. Ciò significa che la mappa non era nella cache oppure che la versione presente nella cache non era aggiornata. Gestione servizi di raccolta quindi recupera la mappa dal server.

Tag	Valore
Severity	1
Event Name	RefreshingMapFromServer
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Aggiornamento della mappa <nome> con id <ID>dal server

Timeout di aggiornamento della mappa

Questo evento interno viene generato dal lato client del servizio di mappatura, ovvero il servizio che fa parte di Gestione servizi di raccolta. Quando in Gestione servizi di raccolta viene ricevuta l'istruzione di aggiornamento della mappatura in seguito a modifiche sopraggiunte o al cambiamento della relativa definizione, viene generato un evento interno. Ciò significa che in Gestione servizi di raccolta si è tentato di recuperare la mappa dal server, ma il server non ha mai ricevuto la richiesta e ha raggiunto il timeout. Questo errore è transitorio e pertanto l'operazione verrà ripetuta in Gestione servizi di raccolta.

Tag	Valore
Severity	4
Event Name	TimeoutRefreshingMap
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	La richiesta ha raggiunto il timeout durante l’aggiornamento della mappa <nome>: <eccezione>

Errore di aggiornamento della mappa

Questo evento interno viene generato dal lato client del servizio di mappatura, ovvero il servizio che fa parte di Gestione servizi di raccolta. Quando in Gestione servizi di raccolta viene ricevuta l'istruzione di aggiornamento della mappatura in seguito a modifiche sopraggiunte o al cambiamento della relativa definizione, viene generato un evento interno. Ciò significa che si è verificato un errore imprevisto e non transitorio durante il tentativo di aggiornamento di una mappa. Gestione servizi di raccolta attenderà 15 minuti e ripeterà l’operazione. Se l’errore si verifica durante l’inizializzazione, il processo continuerà e la mappa sarà ignorata fino a quando non verrà caricata completamente.

Tag	Valore
Severity	4
Event Name	ErrorRefreshingMapData
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Errore di aggiornamento della mappa <nomeMappa>: <exc>

Caricamento mappa di grandi dimensioni

Questo evento interno viene generato dal servizio di mappatura e informa che in Gestione servizi di raccolta è stata caricata una mappa di grandi dimensioni. Una mappa è considerata di grandi dimensioni se comprende più di 100.000 righe.

Tag	Valore
Severity	0
Event Name	LoadedLargeMap
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Il caricamento della mappa <nome> con ID <ID> e <num> voci e dimensioni totali di <#>Kb è stato completato in <##>secondi

Caricamento della mappa di durata eccessiva

Questo evento interno viene generato dal servizio di mappatura e informa che il tempo richiesto per il caricamento di una mappa è eccessivo (superiore a un minuto).

Tag	Valore
Severity	0
Event Name	LongTimeToLoadMap
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	Il caricamento della mappa <nome> con ID <ID> e <num> voci e dimensioni totali di <##>Kb è stato completato in <##>secondi

TimedoutWaitingForCallback

Quando in Gestione servizi di raccolta è necessario aggiornare una mappa, viene inviata una richiesta al backend. Questa richiesta contiene un callback. Il backend genera la mappa che viene inviata a Gestione servizi di raccolta tramite il callback. Se il tempo di risposta è troppo lungo (oltre dieci minuti), Gestione servizi di raccolta invierà una seconda richiesta presumendo che la prima non sia arrivata a destinazione. Quando ciò si verifica, viene generato l'evento interno seguente.

Tag	Valore
Severity	2
Event Name	TimedoutWaitingForCallback
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	La mappa <nome> ha raggiunto il timeout nell'attesa di ricevere il callback con nuovi dati; l'operazione viene ripetuta

ErrorApplyingIncrementalUpdate

Quando nel servizio di mappatura non è possibile applicare un aggiornamento a una mappa client esistente, viene inviato questo evento.

Tag	Valore
Severity	4
Event Name	ErrorApplyingIncrementalUpdate
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	L'errore <errore> si è verificato durante l'applicazione di aggiornamenti alla mappa <nomeMappa> (ID <IDmappa>) v.<versione>. L'aggiornamento della mappa viene ripianificato.

OutOfSyncDetected

Quando nel servizio di mappatura viene rilevata una mappa obsoleta, viene inviato questo evento. Il servizio di mappatura pianificherà automaticamente un aggiornamento.

Tag	Valore
Severity	2
Event Name	OutOfsyncDetected
Resource	MappingService
SubResource	ReferentialDataObjectMap
Message	È stato rilevato che nella mappa <nomeMappa> i dati sono obsoleti, probabilmente perché la notifica di aggiornamento non è stata ricevuta; l'aggiornamento viene ripianificato

Router eventi

Router eventi in esecuzione

Il router eventi è il componente principale di Gestione servizi di raccolta, ovvero quello che esegue le mappe, applica i filtri globali e pubblica gli eventi. Quando il router eventi è pronto per l'esecuzione durante l'inizializzazione, viene inviato questo evento interno. Quando si riavvia Gestione servizi di raccolta, viene inviato un altro evento.

L'evento viene inviato solo dopo che il router eventi ha caricato tutti i filtri globali e le informazioni di mappatura.

Tag	Valore
Severity	1
Event Name	EventRouterIsRunning
Resource	AgentManager
SubResource	EventRouter
Message	Completamento dell'inizializzazione del router eventi in modalità <modalità>

Inizializzazione del router eventi

Questo evento viene inviato quando viene avviata l'inizializzazione del router eventi. Il router eventi avvia l'inizializzazione dopo avere stabilito una connessione con il backend (DAS Query).

Tag	Valore
Severity	1
Event Name	EventRouterInitializing
Resource	AgentManager
SubResource	EventRouter
Message	Inizializzazione del router eventi in modalità <modalità>

Arresto del router eventi

Questo evento viene inviato quando nel router eventi viene ricevuta la richiesta di arresto durante la chiusura.

Tag	Valore
Severity	2
Event Name	EventRouterStopping
Resource	AgentManager
SubResource	EventRouter
Message	Arresto del router eventi

Interruzione del router eventi

Questo evento viene inviato quando nel router eventi viene ricevuta la richiesta di arresto durante la chiusura.

Tag	Valore
Severity	2
Event Name	EventRouterTerminating
Resource	AgentManager
SubResource	EventRouter
Message	Interruzione del router eventi

Motore di correlazione

Motore di correlazione in esecuzione

L'utente può interrompere l'attività del motore di correlazione. Lo stato di esecuzione del motore determina se nel processo attivo gli eventi sono elaborati oppure no. Il processo viene avviato nello stato di inattività (arresto) e attende di recuperare la configurazione dal database. Questo evento viene inviato quando il motore modifica lo stato e si attiva.

Tag	Valore
Severity	1
Event Name	EngineRunning
Resource	CorrelationEngine
SubResource	CorrelationEngine
Message	Il motore di correlazione elabora gli eventi.

Arresto del motore di correlazione

Questo evento viene inviato quando il motore modifica lo stato e si ferma.

Tag	Valore
Severity	1
Event Name	EngineStopped
Resource	CorrelationEngine
SubResource	CorrelationEngine
Message	Il motore di correlazione ha interrotto l'elaborazione degli eventi.

Avvio della distribuzione delle regole

Questo evento viene inviato quando nel motore viene caricata correttamente la distribuzione di una regola. Questo messaggio viene inviato indipendentemente dallo stato di esecuzione del motore.

Tag	Valore
Severity	1
Event Name	DeploymentStarted
Resource	CorrelationEngine
SubResource	Deployment
Message	Avvio della distribuzione di <nome>

Arresto della distribuzione delle regole

Questo evento viene inviato quando la distribuzione di una regola viene scaricata dal motore. Questo messaggio viene inviato indipendentemente dallo stato di esecuzione del motore.

Tag	Valore
Severity	1
Event Name	DeploymentStopped
Resource	CorrelationEngine
SubResource	Deployment
Message	Arresto della distribuzione di <nome>

Modifica della distribuzione delle regole

Questo evento viene inviato quando nel motore viene ricaricata correttamente la distribuzione di una regola. Questo messaggio viene inviato indipendentemente dallo stato di esecuzione del motore.

Tag	Valore
Severity	1
Event Name	DeploymentModified
Resource	CorrelationEngine
SubResource	Deployment
Message	Modifica della distribuzione di <nome>

Sorveglianza

Avvio di un processo controllato

Watchdog viene eseguito come servizio, il cui scopo principale consiste nell'assicurare l'esecuzione dei processi Sentinel. Se un processo viene interrotto, il servizio di sorveglianza lo riavvia automaticamente. Questo evento viene inviato quando si avvia un processo.

Tag	Valore
Severity	1
Event Name	ProcessStart
Resource	WatchDog
SubResource	Process
Message	Generazione del processo <NomeProgramma> (<pid>)

Arresto di un processo controllato

Questo evento viene inviato quando si arresta un processo. Se il processo deve essere ripetuto, ovvero se non deve terminare, il livello di Severity è impostato sul valore 5. Se il processo deve essere eseguito una sola volta, il livello di Severity è impostato sul valore 1.

Tag	Valore
Severity	1/5
Event Name	ProcessStop
Resource	WatchDog
SubResource	Process
Message	Processo <NomeProgramma> terminato con il codice <exit_code>

Avvio di un processo di sorveglianza

Se si avvia il processo di sorveglianza, viene generato l'evento interno seguente.

Tag	Valore
Severity	1
Event Name	ProcessStart
Resource	WatchDog
SubResource	WatchDog
Message	Avvio di un processo di sorveglianza

Arresto di un processo di sorveglianza

Se si arresta il processo di sorveglianza, viene generato l'evento interno seguente.

Tag	Valore
Severity	5
Event Name	ProcessStop
Resource	WatchDog
SubResource	WatchDog
Message	Arresto di un processo di sorveglianza

Gestione/Motore servizi di raccolta

Avvio di porte

Quando si avvia una porta, in Gestione servizi di raccolta viene inviato questo evento.

Tag	Valore
Severity	1
Event Name	PortStart
Resource	AgentManager
SubResource	AgentManager
Message	La porta <ID porta> è in funzione

Arresto di porte

Quando si arresta una porta, in Gestione servizi di raccolta viene generato questo evento.

Tag	Valore
Severity	1
Event Name	PortStop
Resource	AgentManager
SubResource	AgentManager
Message	La porta <ID porta> non è in funzione

Interruzione di processi permanenti

Quando nel connettore dei processi permanenti viene rilevato che il processo controllato è stato interrotto, in Motore servizi di raccolta viene inviato questo evento.

Tag	Valore
Severity	5
Event Name	PersistentProcessDied
Resource	AgentManager
SubResource	AgentManager
Message	Interruzione del processo permanente sulla porta <ID porta>.

Riavvio di processi permanenti

Quando nel connettore dei processi permanenti è possibile riavviare il processo controllato interrotto, in Motore servizi di raccolta viene inviato questo evento.

Tag	Valore
Severity	1
Event Name	PersistentProcessRestarted
Resource	AgentManager
SubResource	AgentManager
Message	Riavvio del processo permanente sulla porta <ID porta>.

Servizio eventi

Dipendenza ciclica

Quando in Servizio eventi viene rilevato un ciclo nella definizione degli eventi (nelle dipendenze tra tag create da assegnazioni di mappe di riferimento), viene generato questo evento. Verificare la configurazione degli eventi in Gestione dati Sentinel e risolvere la dipendenza.

Tag	Valore
Severity	5
Event Name	CyclicalDependency
Resource	EventService
SubResource	ObjectAttrInfos
Message	Dipendenza ciclica rilevata nelle trasformazioni di eventi. Verificare la configurazione di eventi.

Visualizzazioni Active Views

Creazione di visualizzazioni Active Views

Quando viene creata una visualizzazione Active Views, in DAS_Binary viene inviato questo evento.

Tag	Valore
Severity	1
Event Name	RtChartCreated
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	Creazione di una nuova visualizzazione Active Views con filtro <filtro> e attributo <attributo> per gli utenti dotati di filtro di sicurezza <filtro di sicurezza>. Raccolta in corso di <n> visualizzazioni Active Views.

Connessione a una visualizzazione Active Views

Quando un utente si connette a una visualizzazione Active Views esistente, in DAS_Binary viene inviato questo evento.

Tag	Valore
Severity	1
Event Name	RtChartJoiningExistingData
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	Connessione a una visualizzazione Active Views esistente con filtro <filtro> e attributo <attributo> per gli utenti dotati di filtro di sicurezza <filtro di sicurezza>. Raccolta in corso di <n> visualizzazioni Active Views.

Rimozione di visualizzazioni Active Views inattive

Quando una visualizzazione Active Views non permanente viene rimossa perché inattiva, in DAS_Binary viene generato questo evento.

Tag	Valore
Severity	1
Event Name	RtChartInactiveAndRemoved
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	Rimozione di una visualizzazione Active Views inattiva con filtro <filtro> e attributo <attributo> per gli utenti dotati di filtro di sicurezza <filtro di sicurezza>. Raccolta in corso di <n> visualizzazioni Active Views.

Rimozione di visualizzazioni Active Views inattive permanenti

Quando una visualizzazione Active Views permanente viene rimossa perché inattiva, in DAS_Binary viene inviato questo evento. Le visualizzazioni Active Views permanenti vengono salvate nelle preferenze dell'utente e scadono dopo alcuni giorni di inattività per default.

Tag	Valore
Severity	1
Event Name	RtPermanentChartRemoved
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	Rimozione di una visualizzazione Active Views inattiva permanente con filtro <filtro> e attributo <attributo> per gli utenti dotati di filtro di sicurezza <filtro di sicurezza>. Raccolta in corso di <n> visualizzazioni Active Views.

Visualizzazioni Active Views rese permanenti

Quando in DAS_Binary viene rilevata una nuova visualizzazione Active Views permanente, viene inviato questo evento. La verifica viene eseguita periodicamente, quindi la creazione dell'evento può avvenire diversi minuti dopo il salvataggio della visualizzazione Active Views nelle preferenze.

Tag	Valore
Severity	1
Event Name	RtChartIsNowPermanent
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	La visualizzazione Active Views con filtro <filtro> e attributo <attributo> per gli utenti dotati di filtro di sicurezza <filtro di sicurezza> è ora permanente.

Visualizzazioni Active Views non più permanenti

Quando in DAS_Binary viene rilevata una visualizzazione Active Views non più permanente, viene inviato questo evento. La verifica viene eseguita periodicamente, quindi la creazione dell'evento può avvenire diversi minuti dopo la rimozione della visualizzazione Active Views dalle preferenze.

Tag	Valore
Severity	1
Event Name	RtChartNotPermanent
Resource	RealTimeSummaryService
SubResource	ChartManager
Message	La visualizzazione Active Views con filtro <filtro> e attributo <attributo> per gli utenti dotati di filtro di sicurezza <filtro di sicurezza> non è più permanente.

Riepilogo

Event Name	Severity	Origine	SubResource	Componente
AuthenticationFailed	4	UserAuthentication	Authenticate	Autenticazione
NoSuchUser	4	UserAuthentication	Authenticate	Autenticazione
TooManyActiveUsers	4	UserAuthentication	Authenticate	Autenticazione
LockedUser	4	UserAuthentication	Authenticate	Autenticazione
UserLoggedOut	1	UserSessionManager	User	Sessione utente
UserLoggedIn	1	UserSessionManager	User	Utente
UserLoggedIn	1	UserSessionManager	User	Utente
MoveArchiveFileFailed	3	*Nome DAS*	ArchiveFile	Evento
InsertEventsFailed	5	EventSubSystem	Events	Evento
OpenArchiveFileFailed	3	*Nome DAS*	ArchiveFile	Evento
WriteArchiveFileFailed	3	*Nome DAS*	ArchiveFile	Evento
SummaryUpdateFailure	4	Aggregazione	Summary	Aggregazione
InsertIntoOverflowPartition	5	EventSubSystem	Events	Evento
EventInsertionIsBlocked	4	EventSubSystem	Events	Evento
EventInsertionResumed	2	EventSubSystem	Events	Evento
EventRouterIsRunning	1	AgentManager	EventRouter	EventRouter
EventRouterInitializing	1	AgentManager	EventRouter	EventRouter
EventRouterStopping	2	AgentManager	EventRouter	EventRouter
EventRouterTerminating	2	AgentManager	EventRouter	EventRouter
ErrorNoSuchMap	4	MappingService	ReferentialDataObjectMap	Mappatura
LoadingMapFromCache	1	MappingService	ReferentialDataObjectMap	Mappatura
RefreshingMapFromServer	1	MappingService	ReferentialDataObjectMap	Mappatura
TimeoutRefreshingMapData	4	MappingService	ReferentialDataObjectMap	Mappatura
ErrorRefreshingMapData	4	MappingService	ReferentialDataObjectMap	Mappatura
LoadedLargeMap	0	MappingService	ReferentialDataObjectMap	Mappatura
LongTimeToLoadMap	0	MappingService	ReferentialDataObjectMap	Mappatura
TimedoutWaitingForCallback	2	MappingService	ReferentialDataObjectMap	Mappatura
ErrorApplyingIncrementalUpdate	4	MappingService	ReferentialDataObjectMap	Mappatura

Event Name	Severity	Origine	SubResource	Componente
OutOfSyncDetected	2	MappingService	ReferentialDataObjectMap	Mappatura
EngineRunning	1	CorrelationEngine	CorrelationEngine	
EngineStopped	1	CorrelationEngine	CorrelationEngine	
DeploymentStarted	1	CorrelationEngine	Deployment	
DeploymentStopped	1	CorrelationEngine	Deployment	
DeploymentModified	1	CorrelationEngine	Deployment	
ProcessStart	1	WatchDog	Process	
ProcessStop	1/5	WatchDog	Process	
ProcessStart	1	WatchDog	WatchDog	
ProcessStop	5	WatchDog	WatchDog	
PortStart		AgentManager	AgentManager	
PortStop		AgentManager	AgentManager	
PersistentProcessDied	5	AgentManager	AgentManager	
PersistentProcessRestarted	1	AgentManager	AgentManager	
SortDependencies	5	EventService	ObjectAttrInfo	EventService
DbSpaceReachedTimeThrshld	0	Database	Database	Evento
DbSpaceReachedPercentThrshld	0	Database	Database	Evento
DbSpaceVeryLow	5	Database	Database	Evento
RtChartCreated	1	RealTimeSummaryService	ChartManager	Visualizzazioni Active Views
RtChartJoiningExistingData	1	RealTimeSummaryService	ChartManager	Visualizzazioni Active Views
RtChartInactiveAndRemoved	1	RealTimeSummaryService	ChartManager	Visualizzazioni Active Views
RtChartPermanentAndRemoved	1	RealTimeSummaryService	ChartManager	Visualizzazioni Active Views
RtChartIsNowPermanent	1	RealTimeSummaryService	ChartManager	Visualizzazioni Active Views
RtChartNotPermanent	1	RealTimeSummaryService	ChartManager	Visualizzazioni Active Views